Pós-Graduação em Ciência da Computação

EUDES DA SILVA BARBOZA

AUTENTICAÇÃO MULTIFATORIAL EM HARDWARE PARA O PROCESSO DE ASSINATURA DIGITAL DA NF-e

Recife
2018

EUDES DA SILVA BARBOZA

AUTENTICAÇÃO MULTIFATORIAL EM HARDWARE PARA O PROCESSO DE ASSINATURA DIGITAL DA NF-e

Este trabalho foi apresentado à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre Profissional em Ciência da Computação.

Área de Concentração: Segurança da Informação

Orientador: Prof. Dr. Manoel Eusebio de Lima.

Recife
2018

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

B239a Barboza, Eudes da Silva
Autenticação multifatorial em hardware para o processo de assinatura digital da Nf-e / Eudes da Silva Barboza. – 2018.
154 f.: il., fig.

Orientador: Manoel Eusébio de Lima.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2018.
Inclui referências, apêndices e anexo.

1. Engenharia da computação. 2. Segurança da informação. I. Lima, Manoel Eusébio (orientador). II. Título.

621.39 CDD (23. ed.) UFPE- MEI 2018-132

EUDES DA SILVA BARBOZA

AUTENTICAÇÃO MULTIFATORIAL EM HARDWARE PARA O PROCESSO DE ASSINATURA DIGITAL DA NF-e

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Aprovado em: 24/08/2018.

BANCA EXAMINADORA

_____

Prof. Dr. Carlos André Guimarães Ferraz
Centro de Informática / UFPE

_____

Prof. Dr. Alberto César Cavalcanti França
Departamento de Estatística e Informática / UFRPE

_____

Prof. Dr. Manoel Eusebio de Lima
Centro de Informática/UFPE
(**Orientador**)

Dedico este trabalho totalmente, ao Deus que abre porta onde não há porta, que me proporcionou esta benção ao ingressar no mestrado acadêmico do CIn/UFPE, o qual sempre esteve do meu lado, nos momentos bons e difíceis, proporcionando inspiração, incentivo e alegria de viver para a conclusão desta jornada acadêmica.

AGRADECIMENTOS

Em primeiro lugar a Deus pelo dom da vida e principalmente pela salvação em seu filho amado Jesus Cristo, o qual me ajudou a ser aprovado em todas as disciplinas.

A minha amada e bela esposa, companheira no tatear de estrelas, Gyseli Patricy Alves Barboza, bem como, também a minha filha Nicolly Alves Barboza, que em momentos difíceis orava por mim.

Em especial quero agradecer aos meus pais, José Barboza e Maria Avanes da Silva Barboza, que me deram o ensinamento necessário para assumir responsabilidade e seguir em frente com meus ideais.

Ao meu irmão e amigo Ênio da Silva Barboza, o qual que me ajudou bastante com este projeto, bem como, em toda minha trajetória acadêmica.

Quero agradecer ao meu colega Paulo Nunes, pela dedicação e ajuda sincera desde o início do curso até a sua conclusão.

Não posso me esquecer de agradece ao meus colegas e companheiros de profissão: professor Dr. Paulo Sérgio Brandão do Nascimento, o qual foi usado por Deus e me ajudou bastante no pré-projeto desta pesquisa; ao meu professor Dr. César França, que proporcionou conhecimentos necessários em suas aulas de metodologia científica na FAFICA; aos professores MSc. Rodrigo Frutuoso Lopes e MSc. Claudio Pereira da Silva, os quais me deram motivação a seguir em frente com esta pesquisa cientifica, para ingressar no mestrado acadêmico do CIn/UFPE.

Ao meu orientador professor Dr. Manoel Eusebio de Lima, que proporcionou a oportunidade de continuar com esta pesquisa cientifica, o qual me ajudou e soube me conduzir durante o desenvolvimento deste trabalho, incentivando posteriormente a ir em frente ao ingresso do meu futuro doutorado.

Aos empresários e funcionários que participaram da pesquisa, mesmo sendo anonimamente, os quais contribuíram bastante na coleta de informações.

E por fim a todos aqueles que contribuíram diretamente ou indiretamente para a formulação desta pesquisa científica.

RESUMO

Cada dia mais a segurança da informação em ambiente computacional e físico torna-se essencial para manter em segurança, as informações de qualquer organização pública ou privada. Neste contexto, observa-se a presença de falhas de segurança em áreas estratégicas, como no processo da assinatura digital, para posteriormente ser emitida a nota fiscal eletrônica (NF-e) e armazenada no servidor da SEFAZ. Neste particular, não se consegue garantir critérios de autenticidade, quando de seu uso por usuários autorizados por empresas, para emissão de tais notas. Sendo assim, este projeto apresenta o processo vigente de emissão da NF-e, adotado atualmente pelas empresas, e propõe uma nova metodologia, mais segura para a emissão de tais notas fiscais, baseada em autenticação multifatorial de *hardware* biométrico em conjunto com a tecnologia *smart card*, destinados exclusivamente para o sistema de assinatura da NF-e, visando eficiência quanto à autenticidade e não-repúdio na informação. Para alcançar tal objetivo, através de referencial bibliográfico e posteriormente experimental, vamos comparar o processo tradicional de assinatura eletrônica da NF-e, o qual utiliza *token* em PC (certificado tipo A1 e com seu respectivo PIN) ou dispositivos de segurança *token* ou *smart card* (certificados tipo A3 e com seu respectivo PIN), regido pelas regras da infraestrutura de chaves públicas brasileira (ICP-Brasil), com a solução proposta. Para se estimar a eficiência do método, será usada, como exemplo, uma avaliação do sistema tradicional de emissão da NF-e, em 20 empresas de pequeno e médio porte, da cidade de Caruaru, Pernambuco. No entanto, 83% dessas empresas não conseguem garantir autenticidade e não-repúdio de uma NF-e emitida, pelo usuário legítimo do certificado digital. Também, 68% destas empresas já teve problemas de não saber responsabilizar de fato, o usuário que emitiu uma NF-e indevidamente.

Palavras-chave: Segurança da informação. NF-e. Certificação Digital (ICP-Brasil). *Smart Card*. Biometria.

ABSTRACT

Every day more information security in computational and physical environment becomes essential to keep safe the information of any public or private organization. In this context, the presence of security flaws in strategic areas, such as the digital signature process, is followed by electronic invoice (NF-e) and stored on the SEFAZ server. In this regard, it is not possible to guarantee authenticity criteria, when used by users authorized by companies, to issue such notes. Therefore, this project presents the current NF-e issuance process, currently adopted by companies, and proposes a new, safer methodology for the issuance of such invoices, based on biometric hardware multifactor authentication in conjunction with smart technology card, intended exclusively for the NF-e signature system, aiming at efficiency in authenticity and non-repudiation of information. To achieve this goal, through a bibliographic reference and later experimental, we will compare the traditional electronic signature process of NF-e, which uses a token in PC (certificate type A1 and with its respective PIN) or security devices token or smart card (certificates type A3 and with their respective PIN), governed by the rules of the Brazilian public key infrastructure (ICP-Brasil), with the proposed solution. In order to estimate the efficiency of the method, an evaluation of the traditional NF-e emission system will be used as an example in 20 small and medium-sized companies in the city of Caruaru, Pernambuco. However, 83% of these companies fail to guarantee authenticity and non-repudiation of an NF-e issued by the legitimate user of the digital certificate. Also, 68% of these companies already had problems of not knowing how to actually hold the user who issued an NF-e wrongly.

Keywords: Information Security. NF-e. Digital Certification (ICP-Brazil). Smart Card. Biometrics.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AFIS	*AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM*
APDU	*APPLICATION PROTOCOL DATA UNITS*
API	*APPLICATION PROGRAMMING INTERFACE*
ATR	*ANSWER TO RESET*
EEPROM	*ELECTRICALLY-ERASABLE PROGRAMMABLE READ-ONLY MEMORY*
FAR	*FALSE ACCEPTANCE RATE*
FRR	*FALSE REJECTION RATE*
GSM	*GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS*
ISSO	*INTERNATIONAL ORGANIZATION FOR STANDARDIZATION*
JCDK	*JAVA CARD DEVELOPMENT KIT*
JCRE	*JAVA CARD RUNTIME ENVIRONMENT*
JCVM	*JAVA CARD VIRTUAL MACHINE*
JVM	*JAVA VIRTUAL MACHINE*
LDE	LIVENESS DECISION ENGINE
LFD	*LIVE FINGER DETECTION*
OTP	*ONE-TIME PASSWORD*
PIN	*PERSONAL IDENTIFICATION NUMBER*
PSI	*INFORMATION SECURITY POLICY*
PUK	*PERSONAL UNBLOCKING KEY*
RAM	*RANDOM ACCESS MEMORY*
RFID	*RADIO FREQUENCY IDENTIFICATION*
ROM	*READ ONLY MEMORY*
TPDU	*TRANSMISSION PROTOCOL DATA UNITS*

SUMÁRIO

1 INTRODUÇÃO

No Brasil têm sido muito debatidos vários temas relacionados à administração tributária. Dentre destes, pode-se citar a descentralização fiscal, a qual gera pluralidade de rotinas de trabalho, muita papelada, pouca troca de informações entre sistemas de fiscalização e falta de coerência entre as informações econômico-fiscais dos contribuintes (SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO, 2016). Do ponto de vista do cidadão, o estado mostra-se multifacetado, ineficiente e oneroso. Do ponto de vista do governo, o controle tributário apresenta-se difícil pela falta de uma visão integrada das ações dos contribuintes junto ao governo. Em síntese, os custos públicos e privados das obrigações tributárias são elevados. A Carga Tributária Bruta (CTB) de 2016, segundo a Receita Federal do Brasil (2016), subiu nesse ano para 32,38% do Produto Interno Bruto (PIB), atingindo 6.259,23 bilhões de reais, o que impede a geração de novos investimentos e por sequentemente novos empregos (SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO, 2016).

Devido à falta de um controle fiscal mais eficiente, o Brasil deixa de arrecadar mais impostos, como ocorre, por exemplo, com relação ao Imposto sobre Circulação de Mercadorias e Prestação de Serviços (ICMS). Com isso, cada vez mais o governo federal busca informatização de seus processos tributários, visando uma maior integralização, modernização e agilização destes, em um sistema eficaz nos níveis federal, estadual e municipal (PAULINO, 2016).

Como consequência deste processo foi introduzido pelo governo federal, através da Emenda Constitucional n° 42, no Inciso XXII ao art. 37 da Constituição Federal, a definição de que as administrações tributárias (união, estados, distrito federal e municípios) atuem de forma integrada, compartilhando suas informações fiscais, bem como, seus cadastros (TECNOSPEED, 2013).

Como resultado desta iniciativa, foi criada e adotada a nota fiscal eletrônica brasileira (NF-e), a qual, uma vez emitida pela empresa, é automaticamente inserida no sistema da Secretária da Fazenda (SEFAZ). O preenchimento incorreto da NF-e, na tentativa de fraude, ou sua omissão, pode acarretar multas pesadas, que podem variar de 10% a 100% sobre valor da NF-e (MARCHIORO, 2011).

O processo de emissão de uma NF-e requer a utilização de um dispositivo de segurança (*token* em PC, *token* em *hardware* ou *smart card*), em conjunto com sua respectiva senha (também denominada PIN), para a realização da assinatura digital, autorização e encaminhamento dos dados para o servidor da SEFAZ (PORTAL DA NF-e, 2017). No entanto,

embora o processo pareça ser tecnicamente seguro, o fator humano pode provocar um risco em todo o esquema de segurança. Isto ocorre quando existe a falta de autenticidade, ou seja, o reconhecimento correto, ou legítimo, do verdadeiro dono (usuário) do dispositivo de segurança (*token* em PC, *token* em *hardware* ou *smart card*). Por se tratar de dispositivos de segurança portáteis, existe a possibilidade de um funcionário ou invasor se apossar do mesmo e gerar NF-e sem autorização da empresa. Fato este passível de ocorrência devido à maioria dos funcionários de empresas privadas utilizarem para o PIN senhas fáceis, senha padrão de fábrica ou até mesmo seu compartilhamento, desrespeitando a norma de política de segurança de informações (PSI), baseada na ISO 27002:2013. Esta norma deveria ser adotada e também ser de conhecimento de todos os integrantes da empresa (ABNT, 2017).

Em geral, as autoridades certificadoras (AC's), credenciadas pelo órgão maior ICP-Brasil, fazem a sua parte, alertando sobre o uso e a segurança destes certificados no ato da solicitação do mesmo, exigindo a assinatura de um termo de responsabilidade por parte do usuário. Mesmo assim, tais práticas ainda não são suficientes para que o usuário cuide adequadamente de seu *token* ou *smart card*. Frequentemente, estes usuários esquecem o PIN, ou seja, a senha de proteção do certificado digital ou o compartilham, não garantindo que apenas o proprietário real tenha acesso a ele (PATIL, et al., 2017)

Tais irregularidades foram constatadas através de uma pesquisa realizada, como parte deste projeto. Nesta pesquisa foram aplicados questionários e feitas observações durante a jornada de trabalho, em empresas de comércio, escritório de contabilidade, advocacia, entre outros, na cidade de Caruaru, situada no Agreste Pernambucano. Os dados oriundos desta pesquisa foram usados como subsídios para a avaliação deste projeto.

Neste contexto, foi desenvolvido um estudo abordando a análise da nota fiscal eletrônica brasileira (NF-e), visando o desenvolvimento de uma proposta metodológica de autenticação multifatorial de *hardware* biométrico, em conjunto com a tecnologia *smart card*, destinados exclusivamente para o sistema de assinatura da NF-e, objetivando uma maior eficiência em relação aos serviços de autenticidade e não-repúdio, providos pela PSI.

1.1 OBJETIVOS

GERAL

O objetivo geral desta pesquisa é efetuar uma análise do sistema da nota fiscal eletrônica e propor uma melhoria da política de segurança da informação (PSI), para que

somente o detentor legítimo do certificado digital, possa efetuar a assinatura digital da NF-e.

OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral proposto, os seguintes objetivos específicos foram estabelecidos:

- Elaborar revisão da literatura, sobre história da nota fiscal eletrônica (NF-e), bem como, seus benéficos providos para: administrações tributárias, sociedade, vendedor e comprador;
- Verificar o padrão de comunicação da NF-e, assim como, investigar suas características de segurança;
- Estudar as formas de segurança em comunicação de dispositivos criptográficos;
- Propor uma melhoria no processo de assinatura eletrônica da NF-e, com a utilização da biometria (impressão digital) integrada com o *smart card*;
- Desenvolvimento de um simulador do ambiente de: emissão de certificado digital tipo A3 por uma AC (Autoridade Certificadora), processo de assinatura digital, emissão da NF-e e sua validação, tanto por uma AC, como também pela SEFAZ.

1.2 ORGANIZAÇÃO DO TRABALHO

O restante da dissertação tem organização descrita a seguir:

- **Capítulo 2:** Aborda-se todo referencial teórico do trabalho, desde a história da nota fiscal eletrônica (NF-e), como também os padrões de comunicações e processos de emissão da mesma. Este capítulo também aborda a criptografia simétrica, assimétrica e algoritmo de resumo (*hash*), bem como, diferentes tipos de dispositivos de segurança, utilizados atualmente no processo da assinatura digital da NF-e, sistema biométricos, e a tecnologia do *java card*.
- **Capítulo 3:** Destaca-se os principais trabalhos relacionados, com a proposta de solução desta pesquisa científica.
- **Capítulo 4:** Neste tópico descreve-se a metodologia que foi utilizada para a realização da pesquisa, quanto: aos fins, aos meios, a forma de abordagem, o universo

e amostra utilizada, a etapa de coleta de dados e a forma que foi feita a análise dos dados.

- **Capítulo 5:** Descreve-se em detalhe toda a proposta de solução sugerida (Autenticação Multifatorial em *Hardware* para o Processo de Assinatura Digital da NF-e), apresentando-se de forma detalhada todos os módulos de simulação desenvolvidos, uma análise detalhada dos resultados apresentados, comparação com tecnologias existentes, seu impacto e benefícios para o sistema de emissão de NF-e.
- **Capítulo 6:** Neste capítulo são apresentadas as considerações finais quanto à pesquisa, suas limitações e sugeridos trabalhos futuros.

2 NOTA FISCAL ELETRÔNICA

Segundo o Portal da NF-e (2017), elaborado pelo Ministério da Fazenda, define-se que a abreviatura de NF-e, significa nota fiscal eletrônica. A NF-e é um documento fiscal eletrônico emitido pelas empresas e armazenado eletronicamente no servidor da SEFAZ através da internet, com a finalidade de documentar uma prestação de serviço ou uma operação de circulação de mercadorias, ocorrido entre as partes, para eventuais fins fiscais posteriores.

Segundo Hintzbergen (2018), a segurança da informação tem que conter os seguintes serviços de segurança da informação: autenticação, autorização, privacidade, integridade, não-repúdio e disponibilidade.

Sendo assim, a NF-e tem validade jurídica, pois só é possível a empresa emitir a NF-e após assiná-la digitalmente, através do seu certificado digital, garantindo assim sua autoria e integridade.

Atrelando os aspectos relatados anteriormente à necessidade de se ter um controle fiscal mais rígido pelo governo federal, este dispositivo fiscal foi criado e definido na Emenda Constitucional nº 42, Inciso XXII, art. 37, que diz:

> As administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, atividades essenciais ao funcionamento do Estado, exercidas por servidores de carreiras específicas, terão recursos prioritários para a realização de suas atividades e atuarão de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio. (PRESIDÊNCIA DA REPÚBLICA DA CASA CIVIL, 2003).

Em 2004, na cidade de Salvador-BA, durante o 1º Encontro Nacional de Administradores Tributários (ENAT), onde estavam reunidas as administrações tributárias (união, estados, distrito federal e municípios) para atender a esta Emenda, foram colocados em pauta, os seguintes encaminhamentos (PORTAL DA NF-e, 2017):

- Maior integração administrativa das três esferas do Governo;
- Padronização e melhoramento da qualidade das informações;
- Baixar custo e diminuir a carga de trabalho operacional durante atendimento;
- Fiscalização mais eficaz;
- Ações fiscais coordenadas e integradas com maior possibilidade de realização;

- Intercâmbio de informações fiscais entre as administrações tributárias (união, estados, distrito federal e municípios) com maior possibilidade de realização;
- Cruzamento de dados;
- Procedimentos uniformizados.

Ainda neste mesmo encontro foram aprovados os seguintes protocolos de cooperação técnica nas áreas do cadastramento (PORTAL ENAT, 2016):

- Projeto do Cadastro Sincronizado;
- Nota Fiscal Eletrônica (NF-e).

Segundo o Portal da NF-e (2017), elaborado pelo Ministério da Fazenda, a NF-e se tornou o primeiro sistema de informação governamental que integra as esferas federais e estaduais, através da interoperabilidade entre seus sistemas de informação e o dos contribuintes.

Após este encontro foi realizado em abril de 2005, em São Paulo-SP, uma reunião técnica do ENAT, em parceria dos Coordenadores e Administradores Tributários Estaduais (ENCAT), onde foram unificados projetos na área de administração tributária (PORTAL ENAT, 2016). Neste mesmo ano foi realizado o segundo evento do ENAT, desta vez em São Paulo-SP, com a participação dos Secretários de Fazenda dos Estados e DF, Secretário da Receita Federal e dos representantes das Secretarias de Fianças dos municípios de cada capital. Como resultado deste encontro, foi assinado, o protocolo do ENAT 03/2005, que estabeleceu o desenvolvimento e implantação da NF-e (PORTAL ENAT, 2016).

Segundo o Portal da NF-e (2017), elaborado pelo Ministério da Fazenda, ficou definido pelo ENCAT em conjunto com a RFB (Receita Federal do Brasil), as mudanças no processo de emissão de nota fiscal modelo 1 e 1A em papel, para emissão por meio eletrônico, bem como, no controle de gestão das informações fiscais.

Estas mudanças trouxeram os seguintes benefícios:

1. Para as Administrações Tributárias:
    - Maior confiabilidade da nota fiscal;
    - Arrecadação aumentada e com isso, diminuirá a sonegação de impostos;
    - Captura de notas fiscais pela fiscalização com redução de custo no processo de controle;
    - Melhor intercâmbio e compartilhamento de informações entre os fiscos;

- Integralização com o Sistema Público de Escrituração Digital (SPED).

2. Para a Sociedade:
   - Relacionamentos eletrônicos padronizados entre as empresas;
   - Utilização de novas tecnologias incentivando o comércio eletrônico;
   - Geração de emprego na prestação de serviços relacionados à NF-e;
   - Substituição de emissão de nota fiscal modelo 1 e 1A em papel por meio eletrônico;
   - Novas oportunidades de negócios relacionados à NF-e.

3. Para o Vendedor (emissor de NF-e):
   - Relacionamentos eletrônicos com fornecedores (B2B);
   - Documentos fiscais com diminuição de custos de armazenagem;
   - Documento fiscal com diminuição de custos de envio;
   - Redução de custo, em relação aquisição de papel e impressão de notas fiscais;
   - Redução de tempo, em relação às fiscalizações em Postos Fiscais de Fronteira;
   - Facilidade e simplificação de obrigações acessórias.

4. Para o Comprador (receptor da NF-e):
   - Diminuição de erros de digitação de escrituração das notas fiscais;
   - Antecipação da recepção da informação da NF-e pela entrega de logística;
   - Relacionamentos eletrônicos com fornecedores (B2B);
   - Não é mais necessário digitar as notas fiscais na recepção de mercadorias.

2.1 PADRÃO DE COMUNICAÇÃO DA NF-e

A NF-e utiliza um conjunto de protocolos e práticas durante a comunicação do emissor (Empresa) com o receptor (SEFAZ). Segundo o Portal da NF-e (2015), em seu manual de Integração – Contribuinte 6.00, define-se que os protocolos são sempre descritos de forma textual na visão do Governo e não do contribuinte. Sendo assim, na visão do emissor (empresa) percebe-se apenas a transmissão da NF-e.

2.1.1 Web services

De acordo com Portal da NF-e (2015), em seu manual de Integração – Contribuinte 6.00, define-se que o padrão de comunicação utilizado pelo sistema de recepção NF-e seja baseado em *web services* (modelo definido por *WS-I basic profile*), no qual utiliza-se a internet como meio físico para a comunicação em conjunto com dois protocolos: o *hypertext transfer protocol secure* (HTTPS) e o *secure sockets layers* (SSL) versão 3.0 com autenticação mútua.

O protocolo SSL versão 3.0 garante um túnel de comunicação seguro dentro da internet e permite a identificação dos envolvidos pela comunicação através de seus certificados digitais.

No sistema de recepção da NF-e, provido pelo servidor da SEFAZ, os *web services* se comunicam com o sistema da empresa através de trocas de mensagens de acordo com o padrão *SOAP* versão 1.2, o qual determina as trocas de mensagens XML no padrão *Style/Enconding: Document/literal* (PORTAL DA NF-e, 2017). Então, baseado na solicitação de cada serviço, conforme tabela 1, a implementação dos *web services* são classificadas em:

- Síncronos – São utilizados durante a solicitação de algum serviço, onde sua resposta é concluída na mesma conexão. Sendo assim, o resultado deste processamento é devolvido para o contribuinte em uma mensagem que sempre termina com resposta afirmativa ou negativa, com exceção dos serviços *web services* de recepção e de retorno de recepção;

- Assíncronos – São utilizados durante a solicitação de algum serviço, em que sua resposta não é concluída na mesma conexão. Sendo assim, quando há uma mensagem de resposta contendo um recibo, o qual informa o recebimento de uma solicitação, o programa do contribuinte (empresa) irá efetuar uma nova conexão com o servidor da SEFAZ para obter a resposta do processamento do serviço solicitado anteriormente.

Tabela 1 – CLASSIFICAÇÃO DOS SERVIÇOS DA NF-e (IMPLEMENTAÇÃO)

Serviços	**Implementação (*Web Services*)**
Recepção de NF-e	Assíncrona
Cancelamento de NF-e	Síncrona
Inutilização de numeração de NF-e	Síncrona
Consulta da situação de atual da NF-e	Síncrona
Consulta do status do serviço	Síncrona
Consulta cadastro	Síncrona

Fonte: MANUAL DE INTEGRAÇÃO – CONTRIBUINTE VERSÃO 6.00 (2015, pág. 15)

Segue abaixo, uma visão geral desta arquitetura de comunicação (contribuinte / SEFAZ), conforme a figura 1.

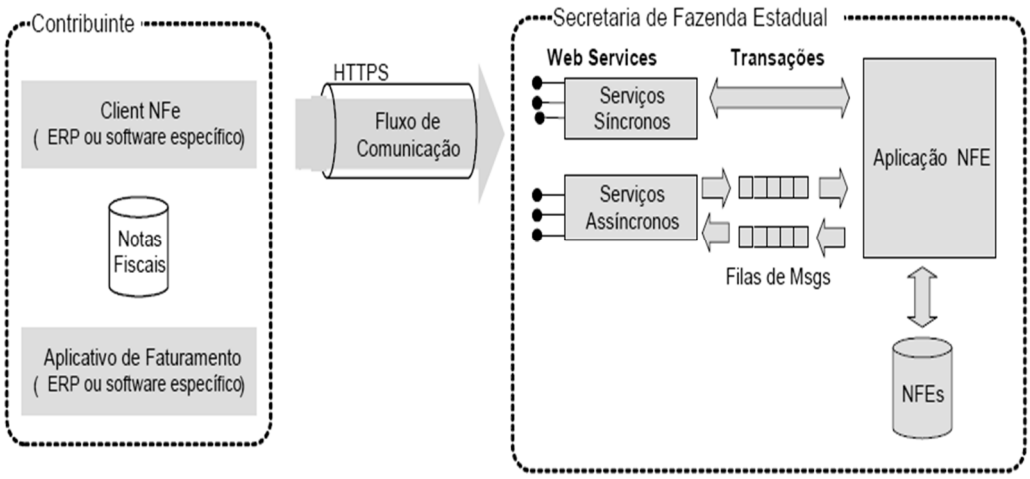


Figura 1 – ARQUITETURA DE COMUNICAÇÃO
Fonte: MANUAL DE INTEGRAÇÃO – CONTRIBUINTE VERSÃO 6.00 (2015, pág. 15)

Na figura 1, referente à arquitetura de comunicação, pode-se visualizar o fluxo de comunicação entre o contribuinte (empresa) e a SEFAZ. O sistema do contribuinte (empresa), sempre inicia a comunicação, enviando uma mensagem por HTTPS com a solicitação do serviço para o *web service*. Após o envio da mensagem, o sistema espera por uma resposta nesta mesma conexão (serviço síncronos), ou para obter o resultado da solicitação do processamento em outra conexão (serviço assíncronos). Neste último, tipo de solicitação, a mensagem fica armazenada em filas de processamento, pois o mesmo requer um tipo de processamento mais intenso (PORTAL DA NF-e, 2015).

2.1.2 Certificado digital

Segundo Machado (2010), nos dias de hoje é essencial segurança da informação para os sistemas computacionais.

Pode-se dizer que um certificado digital é uma ligação entre a chave pública de uma entidade e um ou mais atributos relacionados a esta entidade, armazenados em um arquivo digital. Sendo assim, o mesmo garante que a chave pública pertence a tal entidade e que somente ela possui a correspondente chave privada (MOUTA, 2015).

A certificação digital pode ser utilizada para várias finalidades, como por exemplo, no controle de acesso a recursos, assinaturas de mensagens de correio eletrônico, entre outros. Porém, será abordado aqui apenas o uso da certificação digital para o projeto da NF-e.

Neste contexto, em 1993, o padrão X.509 v1, modelo de infraestrutura de chaves públicas, foi atualizado para a versão v2, na qual foi inclusa dois novos campos usados exclusivamente para controle de acesso. Em 1996 este padrão passou a ser o X.509 v3, na qual foi inserida uma nova versão de campos de extensão (SILVA, et al., 2008). Vale lembrar que:

> O formato X.509 é um padrão de formato de certificado criado pela *International Telecommunication Union – Telecommunication Standartization Sector (ITU-T)* e *ISO/International Electrotechnical Commission (IEC)*, primeiramente publicado em 1988. (SILVA, et al., 2008)

O governo brasileiro utiliza, portanto, a certificação digital baseada no modelo de infraestrutura de chaves Públicas X.509 v3 e adotou seu sistema governamental brasileiro, denominado ICP-Brasil, o qual foi instituída pela medida provisória 2.200-2 de 24 de agosto de 2001. Esta medida tinha como objetivo regulamentar as atividades de certificado digital no país e aumentar a segurança nas transações eletrônicas, como também, incentivar negociações utilizando a internet (presidência da república, 2001).

Segue abaixo, conforme a figura 2, um certificado digital no padrão X.509 v3.

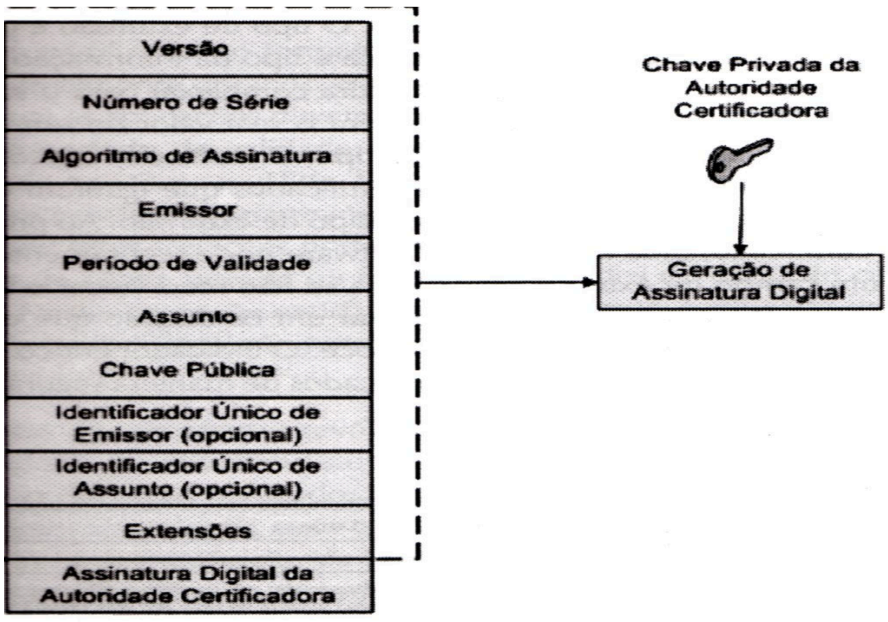


Figura 2 – CERTIFICADO DIGITAL NO PADRÃO X.509 V3

Fonte: SILVA, ET AL., (2008, pág. 27)

De acordo com Ribeiro (2004), define-se que Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) é como um conjunto de entidades, regulamentos e padrões técnicos desenvolvidos para funcionar em sistemas criptográficos com base em certificados digitais.

A ICP-Brasil é uma Autoridade Certificadora (AC) raiz, a qual credenciou algumas AC's intermediárias para emitir certificado digital tipo A1 ou A3 para os usuários, como é o caso da empresa Certisign, Safenet e entre outras (ITI, 2018).

Segue-se abaixo, na figura 3, a hierarquia da ICP-Brasil.

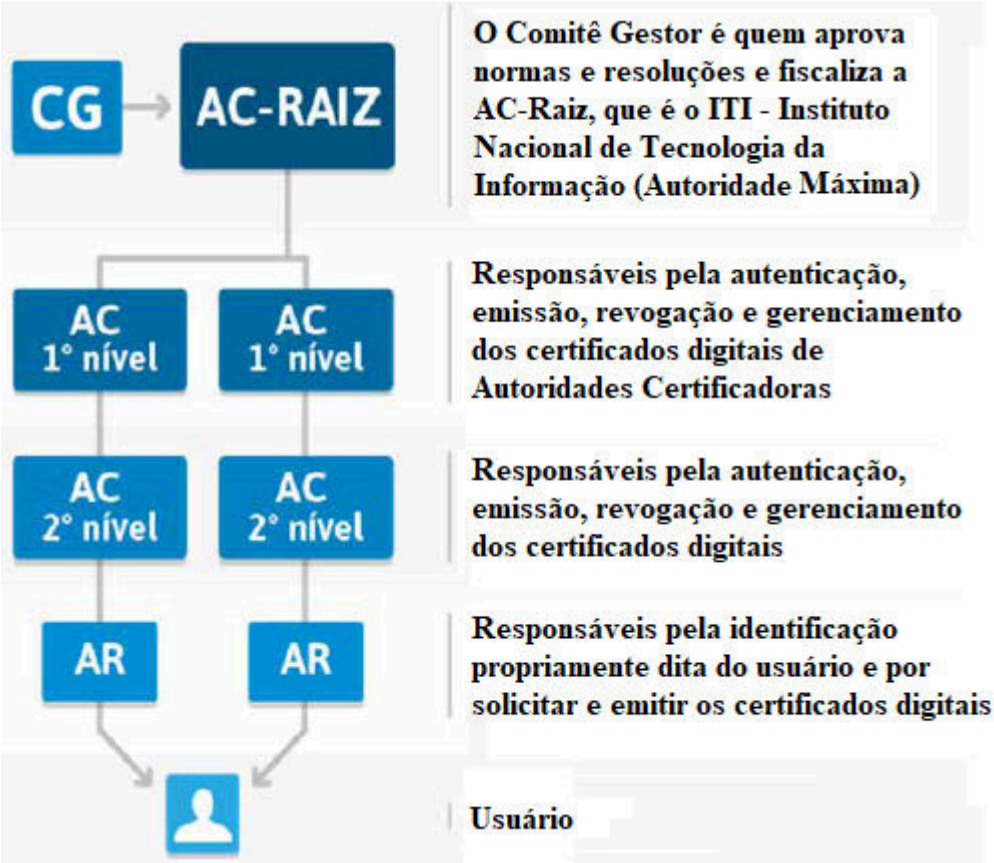


Figura 3 – HIERARQUIA DA ICP-BRASIL

Fonte: ZUNINO, 2017

Em seguida são descritas as garantias oferecidas pela ICP-Brasil aos titulares e usuários de certificados, de acordo com Silva (2008):

- Todas as entidades componentes da ICP-Brasil são obrigadas a contratar seguro, para cobertura de responsabilidade civil compatível com o risco decorrente das atividades de certificação digital e de registro;
- Todas as entidades componentes da ICP-Brasil são obrigadas a declarar todas suas práticas de segurança utilizada, em repositório público para a AC raiz (ICP-Brasil);

- Todas as entidades componentes da ICP-Brasil estão sujeitas a uma auditoria anual prévia para manter-se credenciadas pela ICP-Brasil;
- Todas as entidades credenciadas pela ICP-Brasil tem que possuir padrões de segurança internacional em relação à segurança lógica, física e de pessoal;
- São utilizados algoritmos criptográficos e tamanhos de chaves, os quais são baseados em padrões internacionais para os certificados, mantendo assim um nível de segurança aceitável internacionalmente;
- Deve ser gerado sempre o par de chaves criptográficas pelo próprio titular, onde sua chave privada de assinatura é de seu exclusivo controle, conhecimento e uso;
- Para comprovar e diminuir dúvidas quanto a autenticidade da assinatura do documento, os todos os dados relativos aos certificados são guardados, atendendo assim, as legislações especificas;
- A validação presencial do titular é obrigatória, para obtenção de um certificado digital;
- Todos os documentos assinados com processo de certificação da ICP-Brasil possuem presunção de validade jurídica.

De acordo com o Portal da NF-e (2015), em seu manual de Integração – Contribuinte 6.00, o certificado digital tipo A1 ou A3 tem que conter no campo *otherName* OID=2.16.76.1.3.3 o CNPJ da pessoa jurídica do titular do certificado digital.

De acordo com Mouta (2010), estes tipos de certificados digitais utilizados no Projeto da NF-e são assim definidos:

- Certificado tipo A1 – É um certificado baseado em *software*, onde a AC fornece ao usuário um arquivo em formato criptográfico (certificado digital). Este certificado contém a chave pública e a chave privada, e deverá ser instalado no computador do usuário. Um dos formatos padrão deste arquivo criptográfico é o *PKCS#12* (*Public Key Cryptography Standard*), o qual pode ser reconhecido pela extensão " PFX".
- Certificado tipo A3 – É um certificado baseado em *hardware*, onde a AC fornece ao usuário o certificado digital contendo as chaves (pública e privada), o qual é gerado pelo próprio titular e armazenado em um cartão inteligente (*smart card*) ou em um *token* criptográfico (*token* em *hardware*) inviolável. Os dispositivos de segurança (*token* em *hardware* e *smart card*) possuem um *personal identification number* (PIN) e um *personal unblocking key* (PUK) por questões de segurança. Se o usuário exceder

um número de tentativas de digitação do PIN com erro, o mesmo é bloqueado. Neste caso, o usuário terá que utilizar o PUK para desbloquear o PIN. Porém, se este exceder o número de tentativas de digitação do PUK, o mesmo também é bloqueado, fazendo com que o dispositivo de segurança fique inutilizado. A figura 4, apresenta o fluxo de procedimento para solicitação de um certificado digital tipo A3, adotado por todas AC's.

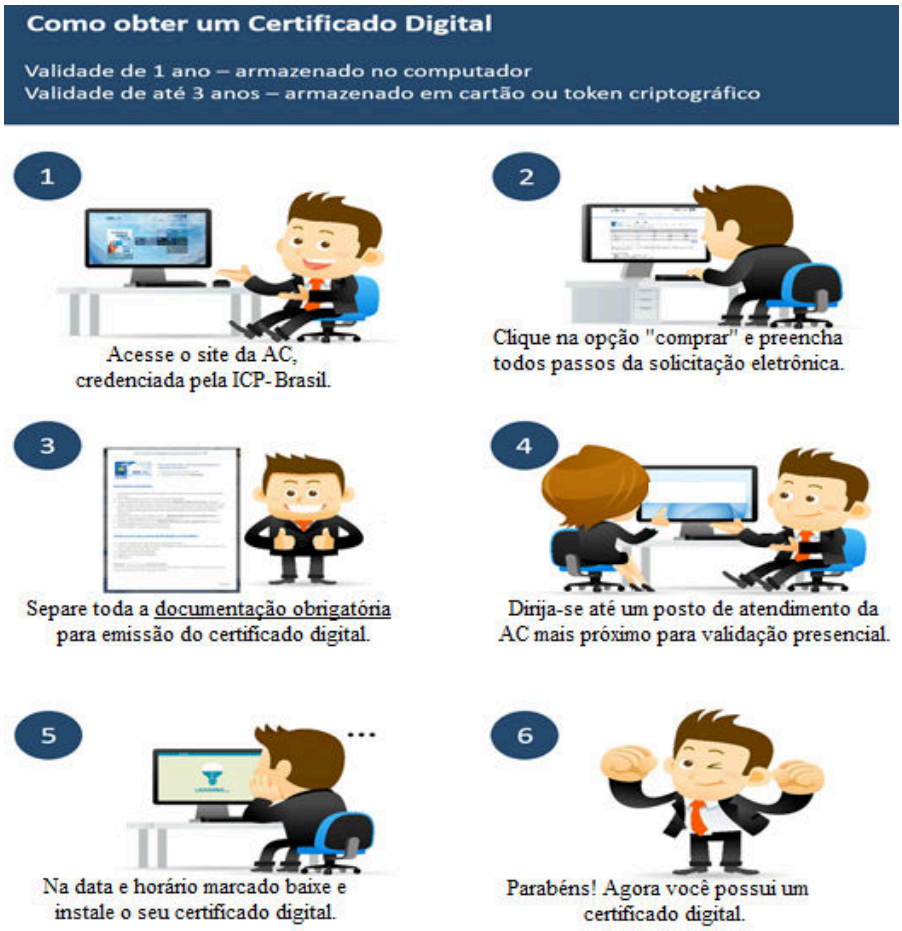


Figura 4 – OBTER UM CERTIFICADO DIGITAL

Fonte: FIGURA REALIZADA PELO AUTOR, BASEADA EM SAFEWEB (2015)

No Projeto da NF-e são exigidos, em dois momentos distintos, os certificados digitais:

1. Para assinatura de mensagens de pedido de cancelamento de NF-e, pedido de autorização de uso, pedido de inutilização de numeração de NF-e e demais arquivos XML que necessitem de assinatura digital. Vale informar que o uso da chave será utilizado para a função de assinatura digital das mensagens, obedecendo assim, aos critérios da política de certificação. O certificado digital deverá conter o CNPJ do titular do mesmo.

2. Durante a transmissão de mensagens entre o programa da empresa com o Portal da Secretaria de Fazenda Estadual. Neste processo o certificado digital do contribuinte deverá conter o CNPJ do emissor das mensagens, e a extensão *Extended Key Usage* com permissão de "Autenticação Cliente".

2.1.3 Assinatura digital

Segundo o Portal da NF-e (2015), em seu manual de Integração – Contribuinte 6.00, menciona-se que durante o processo de emissão da NF-e há utilização da assinatura digital. Segundo Mouta (2015), define-se que a assinatura digital é um conjunto de dados que garante a autenticidade e integridade de uma mensagem.

Para isso, os envolvidos (empresa e SEFAZ), utilizam durante a comunicação, suas respectivas chaves privada e pública, ou seja, um par de chaves assimétricas.

Vale informar, que segundo Zochio (2016), existem dois tipos de criptografia por chaves: chave simétrica ou assimétrica. A tabela 2, apresenta um comparativo entre os dois tipos de criptografia por chaves.

Tabela 2 – COMPARATIVO ENTRE AS CARACTERÍSTICAS DA CRIPTOGRAFIA POR CHAVES

Criptografia Simétrica	Criptografia Assimétrica
Um algoritmo e uma chave	Um algoritmo e duas chaves
Usuários compartilham o algoritmo e a chave	Usuários compartilham um par de chaves
Chave secreta	Apenas uma das chaves é secreta
Impossibilidade de decifrar a mensagem	Impossibilidade de decifrar a mensagem
O algoritmo e as amostras do texto cifrado não devem ser suficientes para determinar a chave.	O algoritmo, as amostras do texto cifrado e uma das chaves não devem ser suficientes para determinar a outra chave.

Fonte: PINHEIRO (2008, pág. 12)

A seguir será descrito como é feito o processo de uma assinatura digital (modelo brasileiro) (SILVA, 2008).

A figura 5 apresenta o fluxo do processo de assinatura digital de uma mensagem.

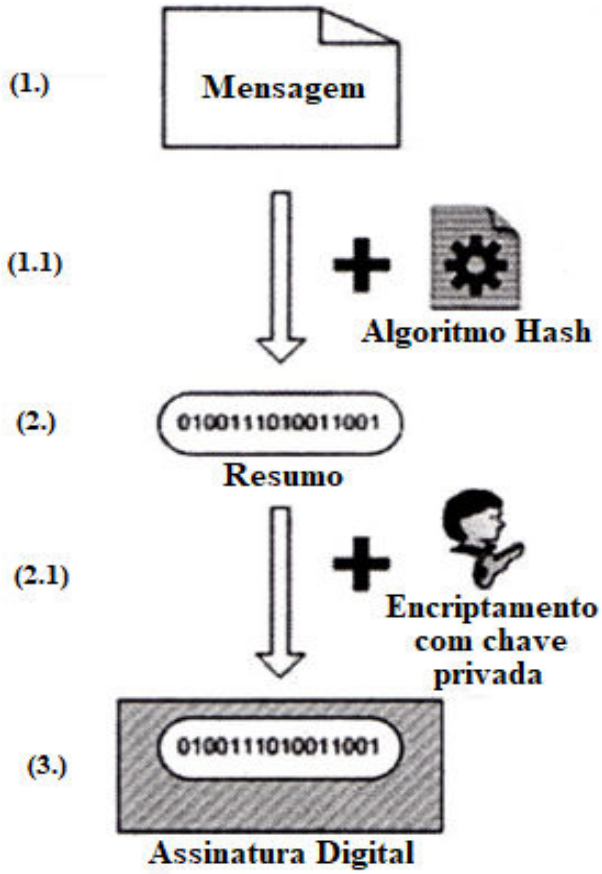


Figura 5 – PROCESSO DE ASSINATURA DIGITAL

Fonte: SILVA, ET AL., (2008, pág. 21)

Na figura 5 percebe-se que são aplicadas três etapas para se concluir o processo de assinatura digital de uma mensagem, quais sejam:

1. Na mensagem é aplicado o algoritmo *hash* (1.1) e com seu resultado, obtém-se um resumo;
2. No resumo é efetuado o encriptamento com a chave privada (2.1) do emitente;
3. Por fim, o resultado deste processo de criptografia, denomina-se assinatura digital.

Quando o emitente envia a mensagem, junto com sua assinatura digital, o destinatário começa a realizar o processo de verificação do mesmo. Este processo serve para verificar se a mensagem não foi alterada durante o percurso, garantindo a integridade dos dados contidos.

A figura 6 apresenta o fluxo do processo de verificação de uma assinatura digital.

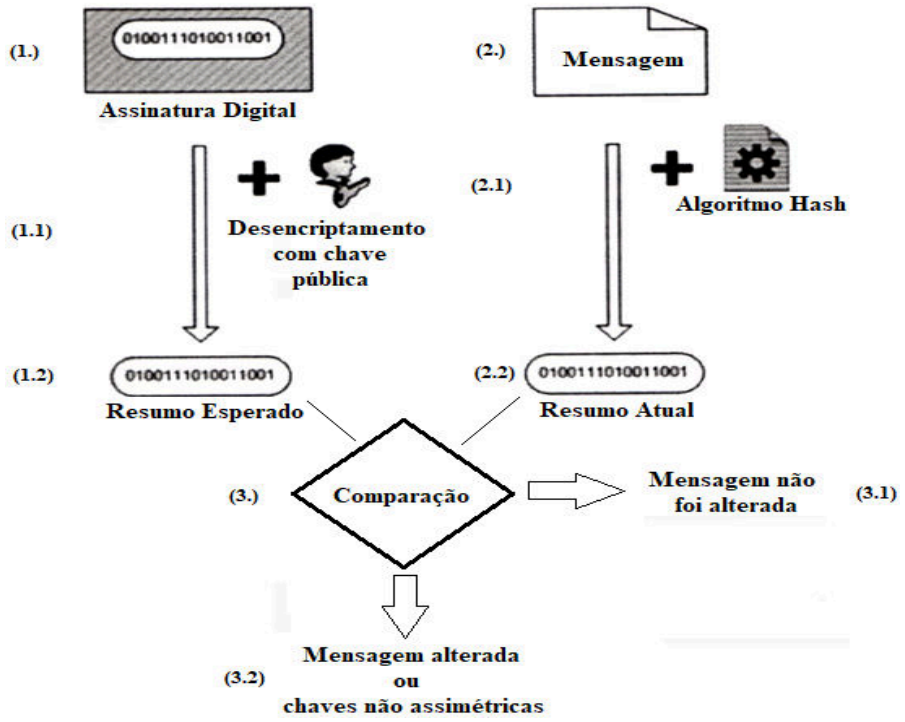


Figura 6 – VERIFICAÇÃO DE UMA ASSINATURA DIGITAL

Fonte: FIGURA REALIZADA PELO AUTOR, ADAPTADA DE SILVA, ET AL., (2008)

Percebe-se que na figura 6 são aplicadas três etapas para conclusão do processo de verificação da assinatura digital, segundo Silva (2008):

1. Na assinatura digital do emitente é efetuado o desencriptamento com a chave pública do mesmo (1.1), para obter o resumo esperado (1.2);
2. Agora na mensagem recebida, o destinatário utiliza-se do algoritmo *hash* (mesmo algoritmo *hash*, que foi utilizado pelo emitente, durante o processo de assinatura digital) e aplica-o (2.1), para obter o resumo atual (2.2);
3. Por fim, é comparado o resumo esperado com o resumo atual. Caso possuam o mesmo valor, então é comprovada que a mensagem não foi alterada (3.1) e a mesma foi assinada digitalmente pelo emitente. Caso contrário, a mensagem foi alterada ou as chaves privada e pública não são assimétricas (3.2).

De acordo com o Portal da NF-e (2015), em seu manual de Integração – Contribuinte 6.00, as mensagens enviadas à SEFAZ são documentos digitais que obrigatoriamente devem estar no padrão XML. Sendo assim, tais documentos digitais em formato XML, devem ser assinados digitalmente com um certificado digital da empresa emissora.

Os padrões que a assinatura digital exige para assinar um documento digital (PORTAL DA NF-e, 2017), são descritos abaixo:

- Padrão de assinatura: "*XML Digital Signature*", utilizando o formato "*Enveloped*";
- Função de "*message digest*": *SHA-1*;
- Certificado digital: emitido por AC credenciada na ICP-Brasil;
- Codificação: *Base64*;
- Cadeia de Certificação: *EndCertOnly* (incluir na assinatura apenas o certificado do usuário final);
- Transformações exigidas: úteis para realizar a *canonicalização* do XML enviado para realizar a validação correta da Assinatura Digital. São elas: (1) *Enveloped* e (2) C14N;
- Tipo do certificado: A1 ou A3;
- Tamanho da Chave Criptográfica: compatível com os certificados A1 e A3 (1024 bits);
- Função criptográfica assimétrica: *RSA*.

2.1.4 Validação da assinatura digital pela SEFAZ

O ENCAT em conjunto com a RFB, determinou as seguintes etapas abaixo, para que a SEFAZ, de cada estado, possa validar uma assinatura digital (PORTAL DA NF-e, 2017):

1. Extrair do certificado a chave pública;
2. Verificar se está dentro do prazo de validade o certificado;
3. Montar e validar a cadeia de confiança de cada certificado, bem como, válida também pela LCR (Lista de Certificados Revogados);
4. Validar o certificado do tipo A1 ou A3, se a chave utilizada está no padrão correto;
5. Garantir que o certificado utilizado é de um usuário final (empresa);
6. Utilizar regras estabelecidas pelo RFC 3280, para as LCR e cadeia de confiança;
7. Serão validadas as LCR utilizadas pelo sistema, a respeito da sua integridade;
8. Verificar o prazo de validade inicial e final de cada LCR utilizada pelo sistema.

Cada Secretaria da Fazenda Estadual (SEFAZ) pode adotar a forma de conferência da LCR de duas maneiras, quais sejam: o *download* periódico ou *download* on-line. Com isso,

todas as mensagens que foram assinadas digitalmente, serão verificadas considerando a LCR disponível no momento da conferência da assinatura.

2.1.5 Processo de emissão da NF-e

Demonstra-se na figura 7, de forma simplificada, o processo de emissão da NF-e, de acordo com o manual de orientação do contribuinte v6.00 (ENCAT, 2015):

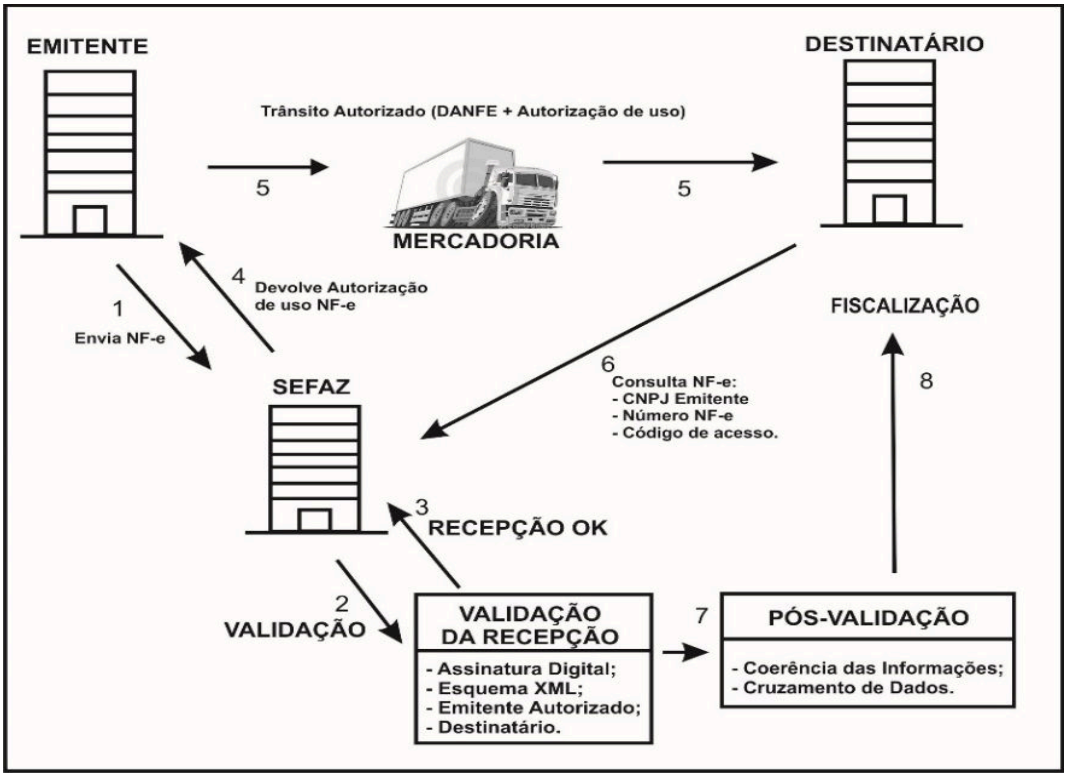


Figura 7 – PROCESSO DE EMISSÃO DE NF-e
Fonte: FIGURA REALIZADA PELO AUTOR

Ainda na figura 7, observe-se que as etapas de 1 a 5, são referentes ao processo de emissão da NF-e. Segue-se as etapas de forma mais detalhada:

1. Quando o emitente (empresa) faz uma NF-e é gerado um arquivo eletrônico (XML), contendo as informações fiscais da operação comercial.

   1.1 Ao tentar-se transmitir este arquivo eletrônico (XML) pela internet, por HTTPS e SSL versão 3.0 com autenticação mútua, para o servidor da SEFAZ (jurisdição do

contribuinte emitente), o próprio aplicativo do emitente solicita a sua assinatura digital.

1.2 Então, para se assinar digitalmente com a chave privada do emitente, é necessário utilizar o dispositivo de segurança (*token* em PC, *token* em *hardware* ou *smart card*) e colocar a sua respectiva senha (PIN), os quais servem para garantir a autoria e a integridade dos dados.

1.3 Após o emitente assinar digitalmente, é anexado o mesmo ao arquivo eletrônico (XML), junto com a chave pública do certificado do usuário final. Em seguida o aplicativo do emitente transmite o arquivo eletrônico (XML) pela internet, por HTTPS e SSL versão 3.0 com autenticação mútua, para o servidor da SEFAZ (jurisdição do contribuinte emitente), utilizando-se assim a tecnologia de criptografia de dados por chave assimétrica.

2. Ao receber o arquivo eletrônico (XML), o servidor da SEFAZ (jurisdição do contribuinte emitente), faz a validação do mesmo. Vale informar que é nesta etapa de validação que o servidor utiliza a chave pública do emitente para descriptografar os dados.

3. Após isto, é enviado o resultado desta validação para o emitente: se a recepção do mesmo estiver tudo OK segue-se para a próxima etapa, se não, uma mensagem de erro é enviada para o aplicativo do emitente, durante o processo de validação.

4. Nesta etapa, a autorização de uso da NF-e é devolvida ao aplicativo do emitente.

5. Com isso, torna-se possível imprimir o DANFE (Documento Auxiliar da Nota Fiscal Eletrônica).

> Para acompanhar o trânsito da mercadoria será impressa uma representação gráfica simplificada da Nota Fiscal Eletrônica, intitulada DANFE (Documento Auxiliar da Nota Fiscal Eletrônica), geralmente em papel comum, em única via. O DANFE conterá impressos, em destaque, a chave de acesso e o código de barras linear tomando-se por referência o padrão CODE-128C, para facilitar e agilizar a consulta da NF-e na Internet e a respectiva confirmação de informações pelas unidades fiscais e contribuintes destinatários. A legislação poderá prever casos em que seja permitida a impressão de mais de uma via do DANFE, como a contingência utilizando formulários de segurança, por exemplo. (ENCAT, 2009).

6. O destinatário, de posse do código de acesso que consta no DANFE, se desejar, pode consultar e confirmar a legitimidade da NF-e, no site da SEFAZ;
7. A SEFAZ de posse do código de acesso, executa uma pós-validação;
8. Por fim é enviado o resultado da pós-validação para o setor de fiscalização.

Após ter sido concluído com sucesso o processo de emissão de NF-e, a própria SEFAZ enviar este arquivo eletrônico para:

- O repositório nacional de todas as NF-e emitidas, que fica no servidor da Receita Federal;
- SEFAZ de destino da operação, no caso se for efetuado uma operação interestadual;
- Entidades e órgãos da administração pública federal direta e indireta, se os mesmos possuírem atribuição legal de regulação, normatização, controle e fiscalização.

2.2 CRIPTOGRAFIA

No ambiente empresarial, a informação é um dos principais ativos, como também é fator decisivo para qualquer empresa se manter em um mercado globalizado e competitivo nos dias de hoje.

Assim, com o ingresso cada vez maior de organizações conectadas às redes de computadores, com seus respetivos sistemas, ficam mais suscetíveis a diversos ataques, ameaças e vulnerabilidades em seus sistemas de informação. Podem-se citar sabotagem, fraudes eletrônicas e entre outras. Tais problemas muitas vezes são causados por códigos maliciosos ou por especialistas em computação (ZOCHIO, 2016). Sendo assim, o que deve ser feito para proteger este ativo tão precioso, que é a informação?

A fim de solucionar este problema, foram desenvolvidas normas de segurança da informação (ABNT, 2017), as quais devem ser de pleno conhecimento para qualquer organização com fins lucrativos ou não. No entanto, apenas conhecê-las não é o suficiente, são necessários que o *chief security officer* (CSO) e o comitê corporativo trabalhem juntos e sempre avaliem o nível de segurança para tal ativo a ser protegido (HINTZBERGEN, et al., 2018).

A família das normas 27000 da NBR ISO (ABNT, 2017), não apenas menciona ativos computacionais, mas também a forma da organização como um todo, onde inclui-se as pessoas que fazem parte da mesma.

Falando sobre segurança da informação em sistemas computacionais, não se pode esquecer de mencionar a criptografia, um dos principais recursos utilizados em certificados de segurança da informação, chamado de *certified information systems security professional* (CISSP), o qual é de porte obrigatório para qualquer profissional CSO, segundo as normas da ISO 27002 (ABNT, 2017).

A definição de criptografia, segundo STEVENSON, et al., (2016), como "*the art of writing or solving codes*", vem dos termos gregos "*kriptos*" que significa "oculto" e "*grafos*" que significa "escrita".

Uma visão sobre a criptografia moderna, em relação à definição de STEVENSON, et al., (2016):

> *This is historically accurate, but does not capture the current breadth of the field or its present-day scientific foundations. The definition focuses solely on the codes that have been used for centuries to enable secret communication. But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic auctions and elections, digital cash, and more. Without attempting to provide a complete characterization, we would say that modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks*. (KATZ, et al., 2014).

Sendo assim, a função da criptografia é de ocultar o significado real da mensagem, já ao contrário da estenografia que é de ocultar a própria mensagem.

Um dos principais sistemas criptográficos históricos é a cifra de César, que se baseia em um método primitivo de cifra de substituição monoalfabética (BONEH, 2017). Pode-se observar seu funcionamento, na figura 8.

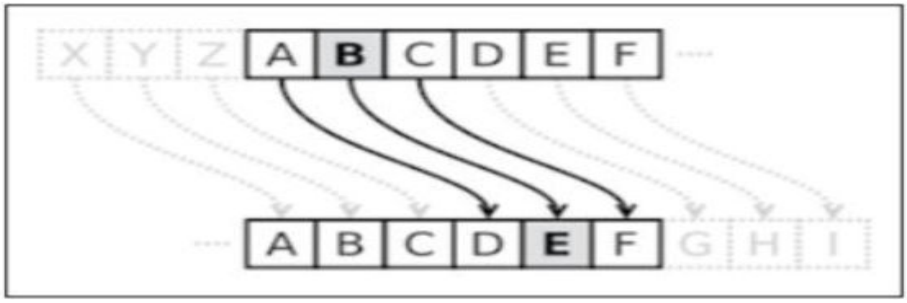


Figura 8 – CIFRA DE CÉSAR
Fonte: SETESYS (2016)

Este método criptográfico, está funcionando com um sistema matemático de deslocamento de 3 posições, para cada letra do alfabeto (mod 26), ou seja:

- Para cifrar podemos usar esta formula C = (P+D) mod 26;
- Para decifrar podemos usar esta formula P = (C-D) mod 26

Onde:

C = Texto cifrado;

P = Texto puro;

D = Chave secreta compartilhada entre as partes, a qual determina a quantidade de deslocamento de posições de cada letra, em um alfabeto com 26 letras “mod 26”.

Note-se que a garantia da eficácia deste método criptográfico, está em guardar em segredo a chave secreta, mencionada na formula acima que seria a sigla D, a qual deve ser só de conhecimento entre as partes envolvidas.

Este método criptográfico da Cifra de César e similares são bastantes frágeis e fáceis de ser decifrado, pois para cada idioma, em seu alfabeto, existe uma tabela que determina a frequência de cada letra que são mais usadas do que outras, conforme o gráfico da figura 9. Sendo assim, é só aplicar um ataque por força bruta e testar as possibilidades do valor de deslocamento da chave secreta compartilhada “D”, até que o texto faça sentido.

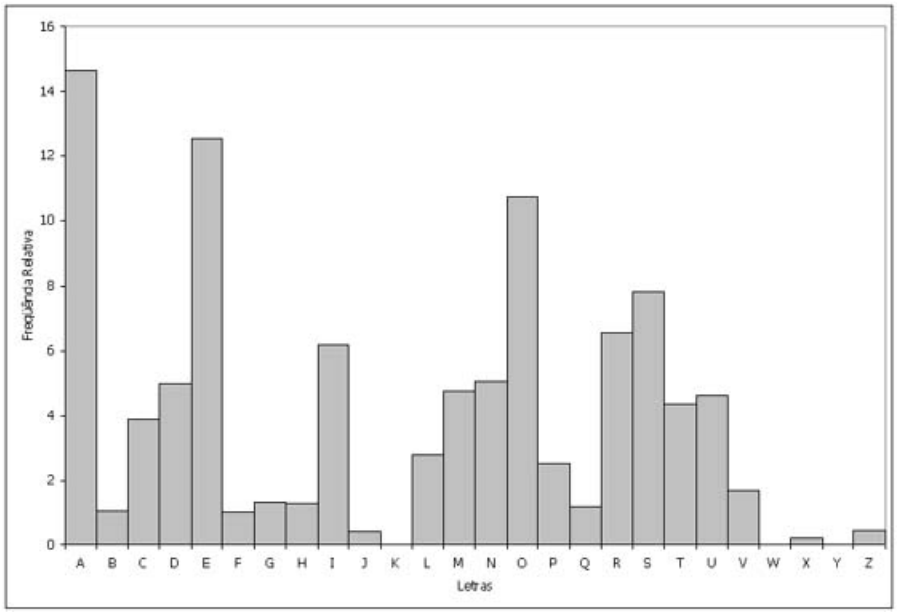


Figura 9 – FREQUÊNCIA DAS LETRAS NO IDIOMA PORTUGUÊS

Fonte: UFRJ (2015)

Existem outros métodos de criptoanálise como: cifra de Vigenère, fórmula final do índice Kappa, bomba de Turing, entre outras (BRAGANÇA, 2017). Sendo assim, tanto a criptografia e a criptoanálise tiveram papel importantíssimo na história sobre as grandes guerras mundiais.

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, e que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De acordo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. (SINGH, 2007).

Nos dias de hoje, mesmo sabendo-se que é o método de transposição é frágil e fácil de ser decifrado, ainda utilizamos o conceito original, só que agora implementamos novas fórmulas matemáticas e algoritmos mais complexos. Com o estudo da entropia na criptografia, se faz necessária obter alguma fonte de dados imprevisíveis para a escolha de um esquema criptográfico perfeito, como por exemplo: confiar em entradas como atrasos entre eventos de rede, tempos de acesso ao disco rígido, pressionamentos de teclas, entre outros, combinados com outras técnicas de geração randômica, fornecendo assim conjunto de dados que tenham entropia suficiente (KATZ, et al., 2014).

Assim, se faz necessário conhecer a abordagem da criptografia clássica e moderna de como seria um esquema criptográfico perfeito, segundo Boneh (2017) e Katz, et al., (2014).

Primeiramente se faz necessário utilizar três algoritmos chamados de: Gen, Enc e Dec, bem como, um espaço de mensagem finito que denominaremos de M, sendo $M > 1$.

O algoritmo Gen é responsável pela geração de chaves probabilísticas, dentro de um espaço-chave finito chamado de K (conjunto de todas as chaves possíveis), no qual produz-se a chave k, de acordo com algum critério de distribuição.

Já o algoritmo de criptografia Enc é responsável por obter como entrada uma chave $k \in K$ e uma mensagem $m \in M$, para que depois seja gerado um texto cifrado, o qual chamaremos de c. Neste algoritmo probabilístico, $Enc_k(m)$ é gerado um texto cifrado diferente, cada vez que for executado. Sendo assim, para indicar o processo de encriptação da mensagem m, usando a chave k (escolhida de forma randômica dentro do conjunto K, de acordo com os critérios estabelecidos) para dar o texto cifrado c, escrevemos $c \leftarrow Enc_k(m)$.

Por último, utilizamos o algoritmo de decriptação Dec, para realizar o processo inverso do algoritmo Enc, ou seja, tendo como entrada uma chave k ∈ K e um texto cifrado c ∈ C, uma mensagem m ∈ M. Neste algoritmo determinístico, Dec_k (c) sempre fornece a mesma saída toda vez que for executado, sem perda de generalidade, sendo assim, escrevemos m: = Dec_k (c) como uma denotação do processo de decriptação do texto cifrado c, utilizando a chave k para produzir a mensagem m.

A figura 10 apresenta o modelo de encriptação e decriptação, descritos anteriormente, a função de cada algoritmo Gen, En e Dec:

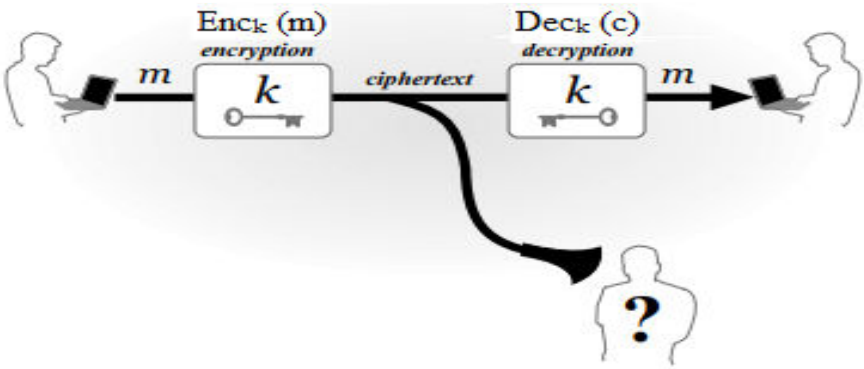


Figura 10 – PROCESSO DE ENCRIPTAÇÃO E DECRIPTAÇÃO
Fonte: FIGURA REALIZADA PELO AUTOR, BASEADA EM KATZ, ET AL., (2014)

Referente ao algoritmo Gen, denota-se Pr [K = k] como a probabilidade de que a saída de K (conjunto de chaves geradas por Gen), seja igual a k, para se obter um segredo perfeito. Sendo assim, deve ser escolhido k de forma aleatória e utilizá-la apenas uma vez, para impedir que o invasor descubra a mesma. De forma M, por ser também uma variável aleatória, denota-se Pr [M = m] como a probabilidade que a mensagem assume o valor m ∈ M.

Ainda baseado na figura 10, vejamos abaixo, o comentário sobre a probabilidade de um atacante, conseguir ou não decrepitar o *ciphertext*:

> *The probability distribution of the message is not determined by the encryption scheme itself, but instead reflects the likelihood of different messages being sent by the parties using the scheme, as well as an adversary's uncertainty about what will be sent. As an example, an adversary may know that the message will either be attack today or don't attack. The adversary may even know (by other means) that with probability 0.7 the message will be a command to attack and with probability 0.3 the message will be a command not to attack. In this case, we have Pr[M = attack today] = 0.7 and Pr[M = don't attack] = 0.3.* (KATZ, et al., 2014)

A seguir são descritos os principais algoritmos simétricos, assimétricos e resumo (*hash*), que são utilizados na criptografia moderna, nos dias atuais.

2.2.1 Algoritmo simétrico

Segundo Boneh (2017), criptografia simétrica são algoritmos que utilizam a mesma chave, tanto para encriptação como também para decriptação de um determinado conjunto de dados. Sendo assim, o mesmo é usado desde 1970 por conta da sua eficácia e rapidez, dependendo do nível de segurança, que a aplicação final exige. A figura 11 mostra um exemplo clássico do fluxo utilizado na criptografia simétrica.

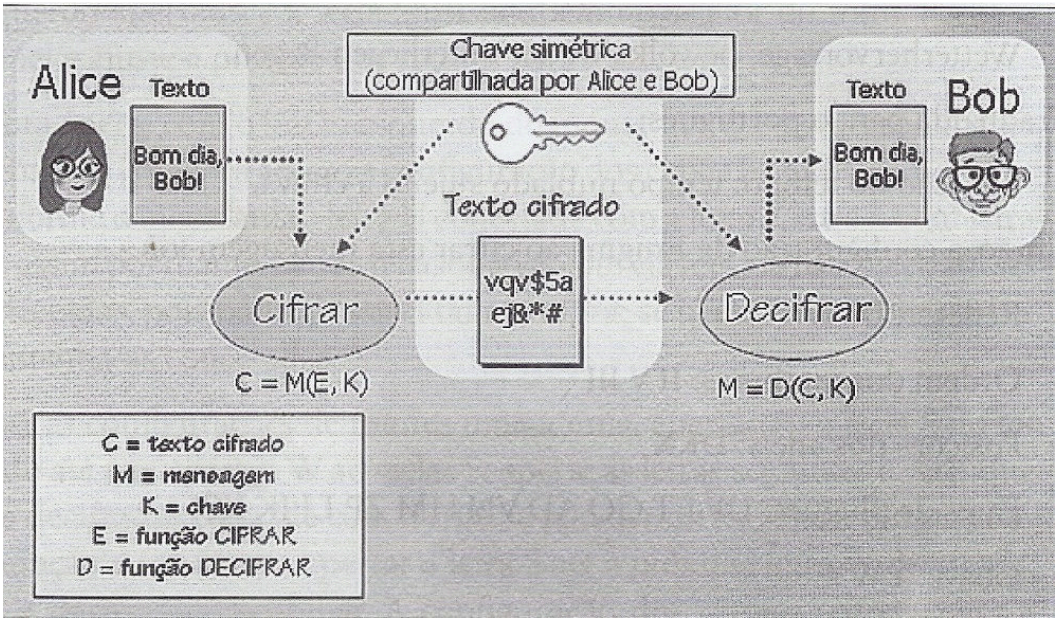


Figura 11 – CRIPTOGRAFIA SIMÉTRICA
Fonte: ZOCHIO (2016, pág. 64)

Observe que na figura 11 se faz necessário utilizar técnicas de segurança para criação de uma sessão de comunicação entre o Alice e Bob, já que a chave simétrica é compartilhada e negociada durante uma sessão.

Em relação à segurança, deve-se levar em conta o tamanho da chave simétrica em bits, pois quanto maior o tamanho da mesma, o algoritmo Gen (geração de chaves simétrica) terá uma maior quantidade de chaves possíveis para serem utilizadas e escolhidas de forma aleatória, durante uma sessão de comunicação.

Por exemplo, tamanho da chave de:

- 40 bits = 2^{40} = 1.099.511.627.776 combinações de chaves;
- 56 bits = 2^{56} = 72.057.594.037.927.936 combinações de chaves;
- 128 bits = 2^{128} = 340.282.366.920.938.463.374.607.431.768.211.4 combinações de chaves.

Sendo assim, só é possível quebrar a criptografia simétrica por ataque de força bruta ou roubando a mesma (KATZ, et al., 2014). Vejamos na tabela 3, o tempo máximo que se leva para quebrar a criptografia simétrica, por ataque de força bruta.

Tabela 3 – FORÇA DA CRIPTOGRAFIA SIMÉTRICA

Tamanho da chave (bits)	Combinações de chaves	Tempo para quebra (1000 chaves geradas/ps)
64	2^{64}	Até 5,1 horas
128	2^{128}	Até 10^{16} anos
256	2^{256}	Até 10^{51} anos

Fonte: BASEADO EM BARROSO (2016)

Um dos algoritmos simétricos mais conhecidos, que utiliza chaves fixas de 56 bits, é o DES (*Digital Encryption Standard*), desenvolvido por Horst Feistel (pesquisador da IBM). Porém, com o avanço tecnológico e com o alto desempenho dos processadores da época em que foram criados, já se era possível, em 1998, quebrar o DES em menos de 3 dias (ZOCHIO, 2016).

Existem vários algoritmos simétricos além do DES, como por exemplo: 3-DES, RC5, Blowfish, CAST-128, IDEA e o AES (BARROSO, 2016). Porém vamos focar no algoritmo AES, o qual foi utilizado no desenvolvimento desta pesquisa.

Desta forma, iniciando com o contexto de criação do algoritmo AES, foi realizado um concurso promovido pelo NIST (*National Institute of Standards and Technology*), o qual elegeu o algoritmo AES (*Advanced Encryption Standard*), desenvolvido pelo belga Rinjdael, como sucessor do DES (ROSA JUNIOR, 2015).

O algoritmo AES foi projetado para resistir e inviabilizar aplicações técnicas em ataques lineares e diferenciais, o qual atualmente se tornou um dos padrões na criptografia de dados em navegadores de internet, pelas seguintes razões (KATZ, et al., 2014):

- Pode trabalhar com tamanho de chaves 128, 192 e 256 bits;

- Utiliza cifragem em blocos de até 128 bits;
- Encriptação e decriptação é mais rápida do que o algoritmo RSA;
- O algoritmo de implementação é público, de acordo com termos da ANSI;
- Sua utilização pode ser tanto em *hardware* como em software.

O modo de operação de qualquer um dos algoritmos simétricos, pode ser em cifra de fluxo ou cifra de bloco.

No modo de cifra de fluxo, utiliza-se uma operação XOR, onde os bits são combinados com os bits do gerador de pseudoaleatórios ou pela própria chave com o texto puro. Deve ser evitado utilizar a mesma chave para encriptar mensagens diferentes. Razão disto, é porque a operação XOR possui propriedades associativa e comutativa, fazendo-se necessário uso de uma chave com tamanho grande em bits, para fornecer ao gerador de chaves AES, um grande conjunto de combinações ou até mesmo combinar com outras técnicas de algoritmos de resumo ou criptográficos. Vejamos um exemplo claro, demonstrado por (ZOCHIO, 2016):

Digamos que duas mensagens A e B, são do mesmo tamanho e que o algoritmo gerador de chaves AES (Gen), escolheu dentro do conjunto K, uma chave que denominaremos de k, a qual será utilizada para encriptar tanto A como B. O modo de operação de cifra de fluxo produz um fluxo de bits C(k), onde a mensagem cifrada ficará assim:

$E(A) = A \oplus C$
$E(B) = B \oplus C$

Se um invasor interceptar E(A) e E(B), pode obter $E(A) \oplus E(B)$. Sabendo que o operador XOR tem propriedade onde $X \oplus X = 0$, logo:

$E(A) \oplus E(B) = (A \oplus C) \oplus (B \oplus C) = A \oplus B \oplus C \oplus C = A \oplus B$

Este processo permite a descoberta do conteúdo da mensagem, mesmo que o texto cifrado tenha tamanho diferente, pois basta truncar o tamanho da mensagem maior “A” e diminuir a mesma para o tamanho da mensagem “B”. Por este motivo se faz necessário utilizar várias técnicas em conjunto e também usar um tamanho de chave maior.

Já no modo de cifra de bloco utiliza-se um algoritmo mais complexo, onde o mesmo efetua operações de substituição e transposição simultaneamente, em cada bloco de tamanho fixo, utilizando a mesma chave k em cada bloco, conforme figura 12.

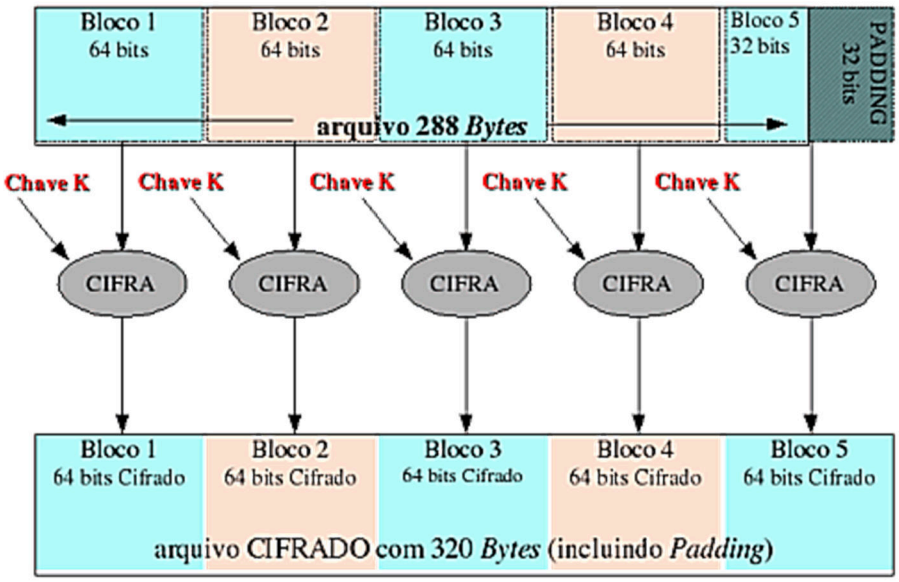


Figura 12 – CIFRA DE BLOCO

Fonte: PROJREDES (2015)

Existem outros modos de operação cifra de bloco, como por exemplo:

- CBC (*Cipher Book Chaining*);
- ECB (*Electronic Code Book*);
- CFB (*Cipher Feedback Block*);
- OFB (*Out Feedback Block*);
- CTR (*Counter*).

Porém, vamos demonstrar apenas o modo de operação CBC (*Cipher Book Chaining*), que foi utilizado no desenvolvimento do projeto. A figura 13 apresenta o modo de operação de encriptação por CBC:

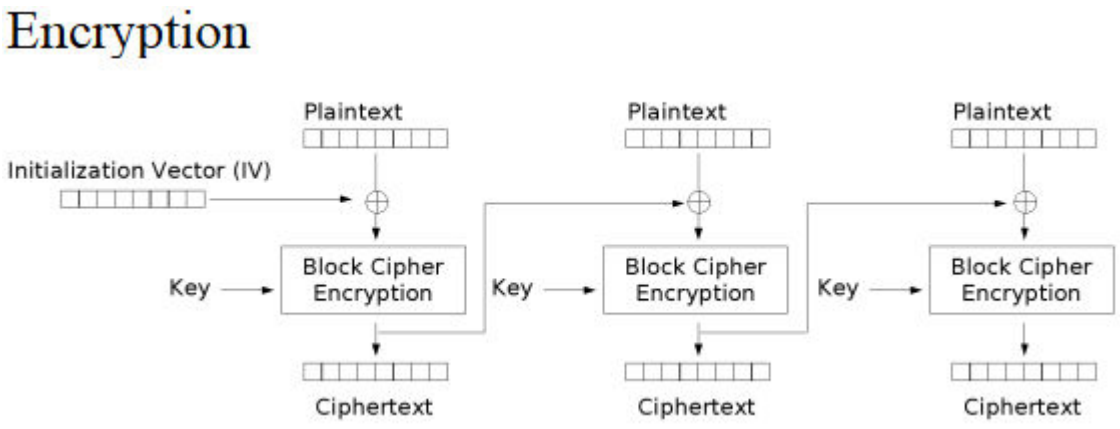


Figura 13 – ENCRYPTION PROCESS (CBC)

Fonte: FIGURA REALIZADA PELO AUTOR, ADAPTADA DE PROJREDES (2015)

Para execução do processo de encriptação (CBC), segue-se as etapas (PROJREDES, 2015):

1. A mensagem original é quebrada em vários blocos *plaintext* de n_b bits. Caso o tamanho da mensagem original não corresponda a um múltiplo do tamanho do bloco *plaintext*, então deve-se aplicar técnicas como *padding* ou *ciphertext stealing*, apenas no último bloco *plaintext*, para preencher n_b bits do mesmo;
2. Deve-se aplicar no bloco *plaintext*, uma operação XOR com seu antecessor de bloco *ciphertext*. Porém, como o primeiro bloco *plaintext*, não possui um antecessor de bloco *ciphertext*, então é executado a operação de XOR, com o bloco *initialization vector* (IV);
3. O resultado da operação XOR, vai para o *block cipher encryption* e posteriormente é aplicado a *key*;
4. Após conclusão da etapa anterior, é gerado como saída o bloco *ciphertext*;
5. Agora o bloco *ciphertext* é utilizado para a próxima operação XOR, do bloco *plaintext* seguinte;
6. Por fim, as etapas 2, 3, 4 e 5, são executadas sequencialmente até que não tenha mais nenhum bloco *plaintext* para ser encriptado. No final de todo o processo, gera-se uma mensagem encriptado.

A figura 14 apresenta o modo de operação de decriptação por CBC:

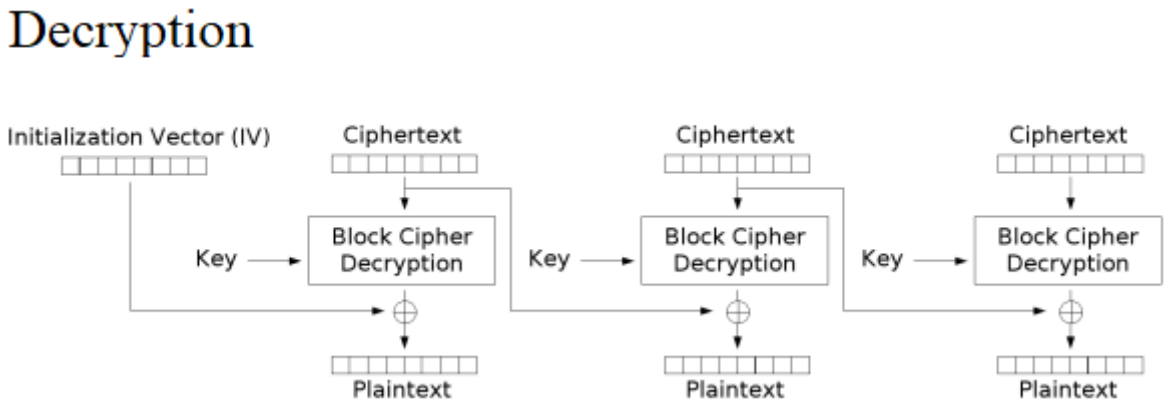


Figura 14 – DECRYPTION PROCESS (CBC)

Fonte: FIGURA REALIZADA PELO AUTOR, ADAPTADA DE PROJREDES (2015)

Para execução do processo de decriptação (CBC), segue-se as etapas (PROJREDES, 2015):

1. A mensagem encriptado é quebrada em vários blocos *ciphertext* de n_b bits;

2. Os blocos *ciphertext* são enviados em paralelo para cada *block cipher decryption* e posteriormente aplicado a key, em cada um;
3. Com o resultado da etapa anterior, aplica-se em cada um, a operação XOR com seu antecessor de bloco *ciphertext*. Porém, como o primeiro bloco *block cipher decryption* não possui um antecessor de bloco *ciphertext*, então é executado a operação de XOR, com o bloco *initialization vector* (IV);
4. Agora com os resultados de cada operação XOR, são gerados os blocos *plaintext*;
5. Por fim, junta-se cada bloco *plaintext* e forma o texto da mensagem original.

No modo de operação CBC, existe uma vulnerabilidade que é o chamado ataque *padding oracle*. Com isso, quando se utiliza o mesmo, deve-se impedir que o servidor da aplicação responda livremente às consultas sobre se a mensagem está corretamente preenchida ou não, para qualquer host ou aplicações ilícitas.

Mesmo cientes da limitação e segurança dos algoritmos simétricos, estes ainda são utilizadas, devido a sua velocidade na hora de encriptar e decrepitar mensagens, independentemente do tamanho destas mensagens. No entanto agora, as aplicações recentes utilizam os mesmos em combinação com outras técnicas de criptografia e codificação, como por exemplo, algoritmo assimétrico, algoritmo de resumo (*hash*), codificação em *base* 64 e entre outros.

2.2.2 Algoritmo assimétrico

O compartilhamento de chave simétrica tornou-se um grande problema para os matemáticos, ou melhor dizer, os criptógrafos, sendo assim, como encontrar uma solução definitiva, para resolver este problema e impedir de uma vez por todas que um atacante consiga descriptografar a mensagem? Ciente deste fato mencionado, os matemáticos e criptógrafos Whitfield Diffie e Martin Hellman, desenvolveram um algoritmo que levou seus nomes, chamado de Diffie e Hellman, de criptografia assimétrica (SILVA, 2017).

Segundo Boneh (2017), criptografia assimétrica são algoritmos que utilizam uma chave pública para encriptação e uma chave privada para decriptação de um determinado conjunto de dados. Sendo assim, estas chaves assimétricas devem ser geradas de forma que serão matematicamente relacionadas, ou seja, números primos.

Segue um exemplo prático, explicado matematicamente, de acordo a ideia de Whitfield Diffie e Martin Hellman (ZOCHIO, 2016).

Digamos que Alice deseja enviar para Bob um arquivo sigiloso, porém ela vai enviar o mesmo por um meio não seguro, que seria os correios, então para garantir que o arquivo sigiloso não seja decifrado por qualquer pessoa, será definido que:

- Arquivo sigiloso de Alice = 10;
- Chave privada de Alice = 15;
- Chave pública de Alice = 15;
- Chave privada de Bob = 20;
- Chave pública de Bob = 20.

Aplicaremos o protocolo, através de uma operação comutável de soma nas etapas a seguir:

1. Alice coloca o arquivo sigiloso dentro de uma caixa e fecha a mesma com um cadeado, chamada A. Assim ter-se-ia 10 + 15 = 25;
2. Agora Alice envia para Bob, a caixa pelo correio sem a chave do cadeado A. A mensagem enviada seria 25;
3. Bob recebe a caixa, porém não consegue abri-la. Bob recebe 25;
4. Bob então coloca na caixa outro cadeado, denominado de B. Agora teríamos 25 + 20 = 45;
5. Em seguida Bob devolve para Alice a caixa pelo correio com o cadeado A e B, porém não envia a chave do cadeado B. A mensagem devolvida seria 45;
6. Ao receber a caixa, Alice abre o cadeado A e devolve a caixa para Bob apenas com o cadeado B. Ou seja, ficaria assim 45 – 15 = 30. Com isso, Alice envia a mensagem = 30 para Bob;
7. Ao receber a caixa, Bob consegue abrir o cadeado B da caixa e finalmente consegue ler a mensagem original (arquivo sigiloso de Alice = 10), pois 30 – 20 = 10.

De acordo com exemplo do protocolo apresentado acima, como é bastante simples, a leitura do arquivo sigiloso poderia ser facilmente comprometida, através de um ataque *man-in-the-middle*. Para evitar tal problema o mesmo foi aperfeiçoado e implementado no algoritmo Diffie e Hellman, que opera com multiplicação e inverso modular, bem como, um gerador de chaves com números primos grandes e difíceis de serem fatorados (KATZ, et al., 2014).

A tabela 4 apresenta o comportamento do algoritmo Diffie e Hellman. Um exemplo do mesmo, é apresentado em seguida para o cálculo da chave secreta (DUARTE, 2016):

Tabela 4 – ALGORITMO DIFFIE-HELMANN

Alice				**Bob**		
Privado	**Público**	**Cálculo**	**Envia**	**Cálculo**	**Público**	**Privado**
A	p, g		p, g →			b
A	p, g, A	$g^a \bmod p = A$	A →		p, g	b
A	p, g, A		←B	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b,s

Fonte: DUARTE (2016)

1. Escolheremos o número primo p = 23 e como base g = 5, para Alice e Bob;
2. Agora Alice escolhe um número secreto a = 6 e envia para Bob $A = g^a \bmod p$;
   $A = 5^6 \bmod 23$
   $A = 15.625 \bmod 23$
   $A = 8$
3. Bob escolhe um número secreto b = 15 e envia para Alice $B = g^b \bmod p$;
   $B = 5^{15} \bmod 23$
   $B = 30.517.578.125 \bmod 23$
   $B = 19$
4. Sendo assim, Alice calcula $s = B^a \bmod p$;
   $s = 19^6 \bmod 23$
   $s = 47.045.881 \bmod 23$
   $s = 2$
5. Depois é a vez de Bob que calcula $s = A^b \bmod p$;
   $s = 8^{15} \bmod 23$
   $s = 35.184.372.088.832 \bmod 23$
   $s = 2$
6. Após estes cálculos, Alice e Bob compartilham uma chave secreta s = 2, porque 6*15 = 15*6.

No exemplo citado acima, Alice e Bob agora só precisam guardar em segredo os valores de a, b e $g^{ab} = g^{ba}$ mod p, porém isto garante uma criptografia segura?

Infelizmente não! Pois se o atacante descobrir os dois números secretos, também será capaz de calcular e descobrir o valor de s. É só aplicar os cálculos abaixo:

- $s = 5^{15*6}$ mod 23;
- $s = 5^{90}$ mod 23;
- s = 807.793.566.946.316.088.741.610.050.849.573.099;185.363.389.551.639.556.884.765.625 mod 23;
- s = 2.

Este fato ocorreu, porque foram escolhidos números pequenos para os valores de a, b e p, ficando assim fácil um ataque por força bruta, a partir do teste de todas as combinações possíveis dos valores de g^{ab} mod 23 até a descoberta do valor de s.

Para uma melhor aplicação das ideias do algoritmo Diffie e Hellman, foi desenvolvido em 1976, pelos professores Ron Rivest, Adi Shamir e Leonard Adleman do MIT (*Massachusetts Institute of Technology*), um algoritmo de criptografia assimétrica que levou as iniciais de seus sobrenomes, chamado de RSA. Este algoritmo mostrou-se capaz de ser aplicado em sistemas reais, e se tornou um dos mais viáveis e seguro usado atualmente (TROTZ, 2005).

O algoritmo RSA se tornou um padrão e referência na criptografia moderna, e é hoje bastante utilizado na maioria dos sistemas computacionais. Ele gera um par de chaves, sendo uma pública e outra privada, onde a chave privada deve ser protegida pelo emissor e a chave pública pode ser de conhecimento de qualquer pessoa.

Na figura 15, podemos observar um fluxo de encriptação do algoritmo RSA.

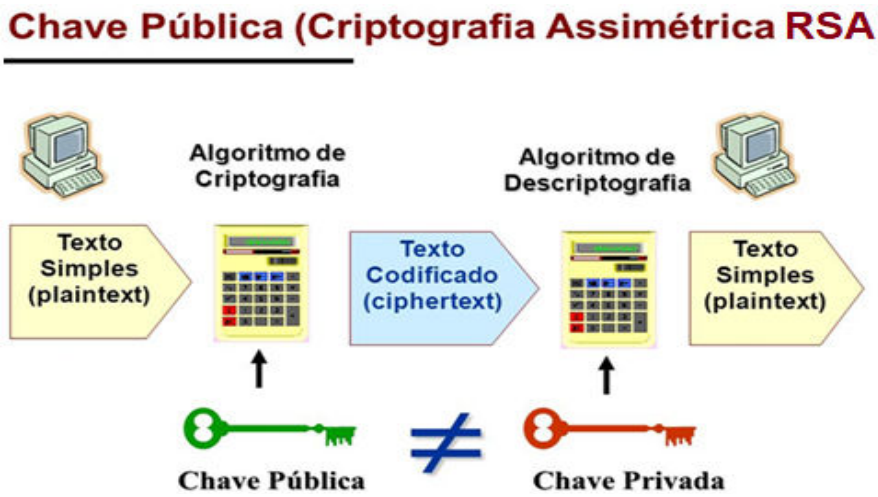


Figura 15 – CRIPTOGRAFIA ASSIMÉTRICA (RSA)

Fonte: JAMHOUR (2013)

Então se Alice quiser enviar uma mensagem para Bob, de forma confidencial, ela utiliza a chave pública de Bob para encriptar o texto simples com o algoritmo RSA e envia para Bob o texto codificado. Então quando Bob recebe o texto codificado, onde ele utiliza sua chave privada para aplicar o desencriptamento com o algoritmo RSA. Com isso, Bob consegue visualizar o texto simples. Da mesma forma que, se Bob quiser enviar uma mensagem para Alice, de forma confidencial, este deve fazer o mesmo procedimento que Alice adotou (BONEH, 2017).

A figura 16, apresenta o fluxo de uma assinatura digital do algoritmo RSA.

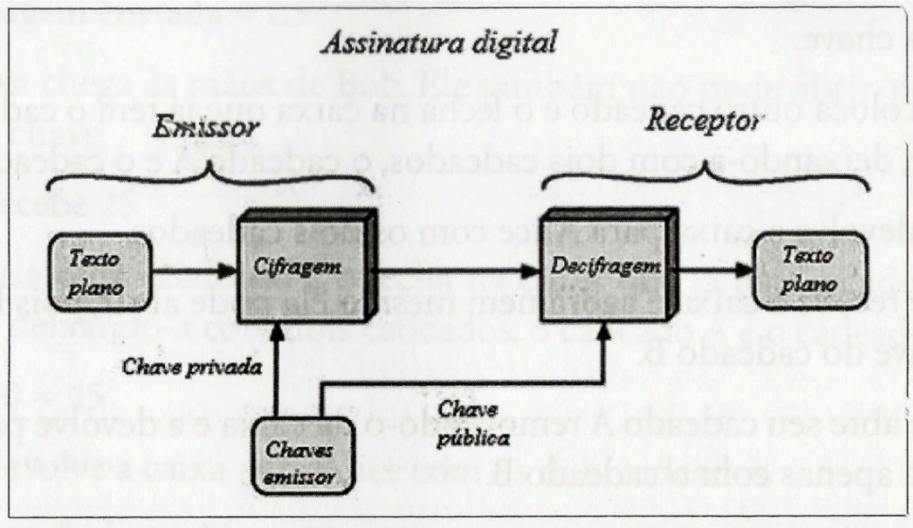


Figura 16 – ASSINATURA DIGITAL
Fonte: ZOCHIO (2016)

Agora, se Alice quiser assinar um documento eletrônico e enviar o mesmo para Bob, de forma que garanta a autoria da mensagem, ela utiliza a sua própria chave privada, em conjunto com o algoritmo RSA e aplica no texto simples. Em seguida envia para Bob o texto codificado. Quando Bob recebe o texto codificado, ele utiliza a chave pública de Alice para aplicar o desencriptamento, em conjunto com o algoritmo RSA e com isso consegue visualizar o texto simples. Da mesma forma que se Bob quiser assinar um documento eletrônico e enviar uma mensagem para Alice, de forma que garanta a autoria da mensagem, deverá fazer o mesmo processo que Alice adotou (BONEH, 2017).

No anexo A, segundo Zochio (2016), demonstra-se dois exemplos de código fonte (linguagem *python*) da criptografia assimétrica RSA, de forma prática e funcional, que calcula os valores das chaves pública e privada, com alguns comentários e o outro código fonte demonstra-se a prova de conceito, para cifrar ou decifrar um texto.

Vejamos abaixo, um comentário sobre a segurança do algoritmo RSA:

> A segurança do RSA depende muito da dificuldade de se fatorar números grandes e dos números primos escolhidos para criar as chaves. A forma mais óbvia de atacar o RSA é descobrir um método de fatoração rápido que consiga abrir n nos seus fatores primos. (ZOCHIO, 2016)

Por este fato mencionado anteriormente é que atualmente utilizamos em sistemas computacionais, cada vez mais, chaves com tamanho de 1024 bits, 2048 bits ou 4096 bits. Vale informa que existe um inconveniente de se utilizar chaves grandes, pois se aumentarmos o tamanho da chave, o sistema de criptografia fica mais seguro, porém por outro lado o processo de encriptação e decriptação fica mais lento, fato este porque o algoritmo RSA é cerca de cem vezes mais lento do que o algoritmo DES. Por este motivo é que o algoritmo RSA é mais utilizado em aplicações de assinatura digital de um arquivo, em conjunto com o algoritmo de resumo (*hash*) (ROSA JUNIOR, 2015).

2.2.3 Algoritmo de resumo (hash)

Devido ao processo de criptografia assimétrica é lento, como visto no algoritmo RSA, é muito comum se utilizar, em assinatura digital, o algoritmo de resumo (*hash*).

Mas, o que é o algoritmo de resumo e qual é sua finalidade?

> Também conhecidos por algoritmos de assinatura digital, estes algoritmos utilizam função *hash* para gerar um valor matemático para uma sequência de dados, mapeando textos plenos de tamanhos variados em um texto cifrado de tamanho fixo. Estes algoritmos são geralmente utilizados para converter mensagens extensas em mensagens menores que representam a mensagem original. (ROSA JUNIOR, 2015)

A figura 17 apresenta um exemplo de utilização do algoritmo de resumo (*hash*), para o processo de assinatura digital de um arquivo.

Figura 17 – FUNÇÃO HASH E ALGORITMO DE CRIPTOGRAFIA ASSIMÉTRICA

Fonte: TOLEDO (2012)

Os algoritmos de resumo (*hash*), mais utilizados na criptografia assimétrica (RSA) são:

- SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512 (*Secure Hash Algorithm*-*);
- MD5 (*Message Digest* *).

Porém, nosso foco é no algoritmo de resumo (*hash*) SHA-1, pois segundo ENCAT (2015) é o padrão adotado pelo processo de assinatura digital da NF-e, e o utilizado no desenvolvimento do projeto.

2.3 DISPOSITIVOS DE SEGURANÇA

No ambiente de certificação digital é necessário utilizar autenticadores. Para isso, existem três tipos de autenticadores (KERBY, 2012):

- Algo que o usuário sabe – É um método que se baseia apenas no conhecimento de algo. Sendo assim, neste método um segredo é compartilhado entre o usuário e o sistema, como por exemplo, uma senha.
- Algo que o usuário possui – É um método que se baseia apenas na posse de um objeto. Sendo assim, neste método o usuário tem que estar de posse de um objeto que foi lhe dado anteriormente pelo sistema para se autenticar, como por exemplo, um cartão de ponto eletrônico.
- Algo que o usuário é – É um método que se baseia apenas nas características biométricas do usuário. Sendo assim, neste método o usuário para se autenticar no sistema, tem que apresentar suas características biométricas, como por exemplo, reconhecimento facial, existentes em caixas eletrônicos.

Para que um sistema seja seguro e válido, é necessário que o mesmo utilize no mínimo dois fatores de autenticação. O uso de dois ou mais destes fatores é conhecido como autenticação de múltiplos fatores (PINHEIRO, 2008). Por isso, o projeto de NF-e exige atualmente autenticação de múltiplos fatores durante a utilização dos certificados digitais que são: algo que o usuário possui e algo que o usuário sabe.

Sendo assim, foram introduzidos os dispositivos de segurança (*token* em PC, *token* em *hardware* ou *smart card*) para a certificação digital. Estes dispositivos são utilizados para fornecer a chave privada, algo que o usuário possui, e em seguida, é solicitado o respectivo PIN, algo que o usuário sabe, para concluir o processo da assinatura digital.

É muito importante escolher bem o tipo de certificado digital junto a AC intermediária que lhe atende. O certificado tipo A1 oferece um melhor desempenho para realizar a assinatura digital em ambientes com uma grande demanda de NF-e, porém o mesmo oferece um nível de segurança, inferior ao tipo A3. O certificado tipo A3 por sua vez, tem um menor desempenho para realizar a assinatura digital em uma grande demanda de NF-e, mas oferece maior segurança em proteger a chave privada e pública do titular, armazenadas em um dispositivo de segurança baseado em *hardware* (MOUTA, 2015).

Neste trabalho, o foco será dispositivos de segurança baseados em *hardware*, especificamente *smart card*.

2.3.1 Token

Segundo Vieira (2007), define-se *token* como um objeto que tem a função de identificar o usuário titular em um sistema computacional.

Um exemplo bem prático da utilização do *token* no nosso dia-a-dia são os antigos cartões de crédito, os quais identificam o usuário da transação por meio deste dispositivo de segurança.

Percebe-se, portanto, que o *token* é um dos dispositivos de segurança mais comuns do mercado e de baixo custo de produção (RUGGIERO, et al., 2007).

Segundo Vieira (2007), existem quatro tipos de *token*:

- *Token* em PC;
- *Token* em dispositivos portáteis;
- *Token* em papel;
- *Token* em *hardware*.

A verificação do *token* é feita por um algoritmo de desafio/reposta de forma implícita ou explícita. Sendo assim, quando o servidor (sistema computacional) propõe um desafio, somente o usuário dono do *token*, é capaz de responder corretamente à solicitação. Serão vistos abaixo, os tipos de desafio que o servidor (sistema computacional) propõe (RUGGIERO, et al., 2007):

- Desafio baseado em eventos – A cada uso do *token* é incrementada uma sequência numérica como desafio;

- Desafio baseado em tempo – O servidor não propõe nenhum desafio. Sendo assim, para que seja utilizado à hora atual como entrada do desafio, faz-se necessário que a hora do servidor (sistema computacional) e do *token* esteja sincronizada;
- Desafio explícito – O usuário utiliza o teclado para responder o desafio do servidor (sistema computacional).

Como o assunto aqui discutido é a NF-e, a qual utiliza certificação digital, então vão ser apresentados a seguir, apenas os dispositivos de segurança *token* em PC (certificado tipo A1) e mais precisamente *token* em *hardware* (certificado tipo A3).

TOKEN EM PC (CERTIFICADO TIPO A1)

Segundo Vieira (2007), define-se *token* em PC como sendo um programa, o qual para ser executado necessita-se que o usuário digite sua senha para acessar suas funcionalidades.

No ambiente de certificação digital para NF-e, as AC's (Autoridades Certificadoras) intermediárias geram no próprio cliente o par de chaves criptográficas dentro do PC (MOUTA, 2010).

O *token* em PC, ou melhor, *token* em *software* pode ser combinado com múltiplos fatores de autenticação e, além disso, possui uma grande vantagem, pois não se faz necessário portar nenhum dispositivo físico. Como seu grande poder computacional está em utilizar os recursos (processador, memória e entre outros) do PC, então, pode-se utilizar algoritmos assimétricos com maior rapidez, como por exemplo, uma grande demanda de assinaturas digitais para as NF-e diárias ou até mesmo operações computacionais mais pesadas (VIEIRA, 2007).

Vale ressaltar que, por conta da chave criptográfica ficar armazenada dentro do PC, a mesma fica vulnerável a ser capturada por algum invasor. Ou seja, se o PC do usuário estiver infectado com algum aplicativo espião (*spyware*), sua identidade digital pode ser comprometida e violada. Por isso é que os certificados tipo A1 são menos seguros (RUGGIERO, et al., 2007).

No processo de emissão da NF-e é utilizado o algoritmo desafio/resposta baseado em desafios explícitos. Sendo assim, o servidor (sistema computacional) verifica no *token* em PC sua respectiva chave privada que está armazenada no PC, a qual usuário está utilizando, e manda um desafio solicitando o PIN do mesmo para concluir a assinatura digital do arquivo XML da NF-e.

TOKEN EM HARDWARE (CERTIFICADO TIPO A3)

Segundo Revistabw (2016), define-se que *token* em *hardware* como sendo pequenos dispositivos, capazes de armazenar chave privada e o certificado digital, com segurança.

Deste ponto em diante o *token* em *hardware*, ou mais precisamente *token* de segurança que utiliza conexão USB e teclado, será simplesmente referenciado como *token*.

No ambiente de certificação digital para NF-e, as AC intermediárias geram no próprio cliente o par de chaves criptográficas dentro do *token*.

Este dispositivo é destinado a ser ligado na porta USB do PC (*Personal Computer*), para entrar em comunicação com o mesmo. Sendo assim, cada vez que se é utilizado o *token* é gerado um novo desafio, ou seja, uma nova OTP (*One-Time Password*) única para cada acesso da comunicação. Vale lembrar que o *token* possui uma vantagem em relação ao *smart card*, pois o mesmo não necessita de nenhuma leitora para funcionar (ZANINI, 2007).

Segue abaixo, conforme a figura 18, o dispositivo de segurança *token*.

Figura 18 – DISPOSITIVO DE SEGURANÇA (TOKEN)
Fonte: CERTISIGN (2017)

O *token* pode ser combinado com múltiplos fatores de autenticação, por exemplo, combinar autenticação por PIN (numérico) e temporização da aplicação, o que o torna vantajoso em tecnologia. O *token* possui um método de isolação especial de seus dados, ou seja, tanto a memória, o algoritmo, a entrada de dados e a chave criptográfica não correm riscos de serem roubados, desde que, as operações e as exibições de dados que forem executados pelo mesmo, ficam isoladas do computador. Com isso, mesmo que o usuário utilize o *token* em um computador que esteja infectado com algum aplicativo espião (*spyware*), sua identidade digital continua inviolada. Por isso, os certificados tipo A3 são mais seguros (RUGGIERO, et al., 2007).

Posteriormente foi desenvolvido pela empresa *Aladim* o *etoken*. Este dispositivo de segurança possui as mesmas características de um *token* normal, porém com uma diferença, o *etoken* agora possui um chip embutido, igual ao que é utilizado pelo *smart card* (SAFENET, 2017). Mesmo assim, tanto o *token* e o *etoken* possuem uma estrutura física de plástico pequena, pela qual não é possível disponibilizar visualmente uma identificação impressa dos dados do usuário.

No processo de emissão da NF-e é utilizado o algoritmo desafio/reposta baseado em desafios explícitos. Desta forma, o servidor (sistema computacional) verifica no *token* sua respectiva chave privada, que o usuário está utilizando, e manda um desafio solicitando o PIN do *token* para concluir a assinatura digital do arquivo XML da NF-e.

2.3.2 Smart card

O que é um *smart card* (cartão inteligente)?

> ... Podemos defini-lo como um cartão de plástico com um chip de computador embutido. O chip pode ser tanto um microprocessador com memória interna - *Microprocessor Card* - ou um chip de memória com lógica não programável - Memory Card. A conexão do chip pode ser tanto via contato físico direto como remotamente via uma interface eletromagnética. (MATOS, 2003).

A tecnologia *smart card* foi desenvolvida entre os anos 70 e 80 por inventores da França, Japão e Alemanha. Já na década de 80 foram desenvolvidas várias maneiras de utilizá-lo em nosso dia a dia, como foi o caso das empresas *France Telecon* e a *French National Visa Debit Card*. Já a *International Standards Organisation* foi quem definiu o padrão para estrutura física do *smart card* pelo padrão ISO 7810, 7816-1 e 7816-2 (MATOS, 2003).

Sua estrutura física é composta de cinco partes, conforme Matos (2003):

1. As dimensões do cartão de plástico são de 85,60mm x 53,98mm x 0,80mm;
2. *Plastic support* – É um suporte de plástico utilizado para acomodar o chip;
3. *Glue* – É um tipo de cola apropriado para fixar o chip;
4. *Microcontroller* – É um chip de micro controlador com cinco pontos de conexão para dados e alimentação, ou seja, o mesmo controla e executa todas as funções do *smart card*;

5. *Printed circuit* – É um circuito impresso que serve como contato de conexão para o leitor se comunicar com *microcontroller*. Sendo assim, este *printed circuit* (circuito impresso) é colocado por cima do *microcontroller*, para proteger o mesmo da eletricidade estática e estresse mecânico.

A estrutura física de um *smart card é mostrada n*a figura 19.

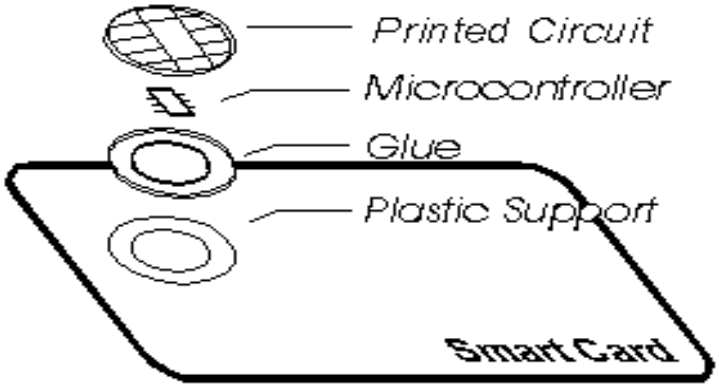


Figura 19 – ESTRUTURA FÍSICA DO SMART CARD
Fonte: MATOS (2003)

O *smart card* é um dos principais dispositivos de segurança na área de certificação digital, capaz de guardar chaves privadas e públicas, informações pessoais, entre outros dados, com total confidencialidade e segurança.

O *printed circuit* é baseado pelo padrão ISO 7816-3 e é composto por: Memória ROM, memória EEPROM, memória RAM e CPU, conforme figura 20 (ISO, 2016):

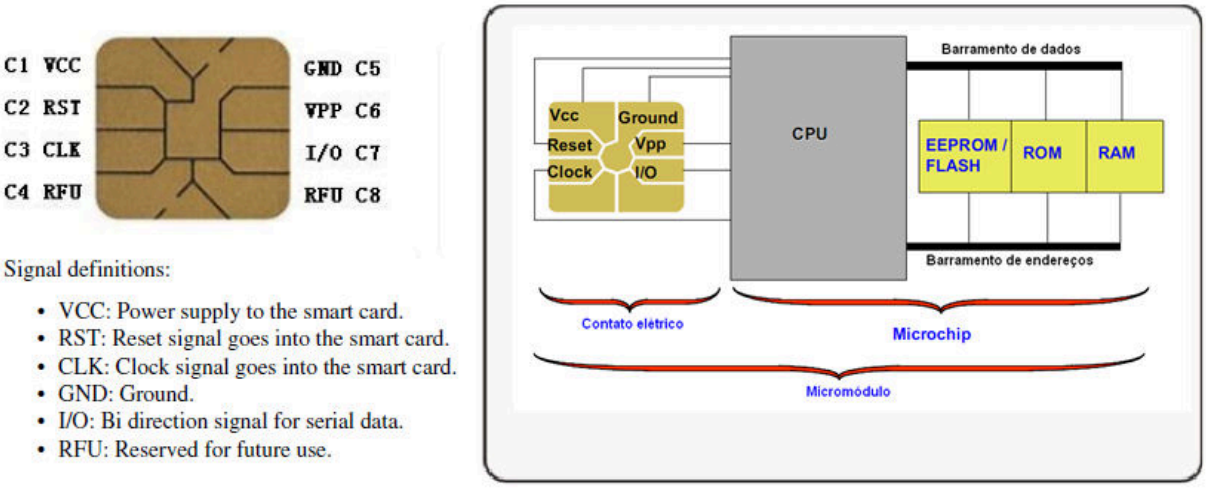


Figura 20 – PRINTED CIRCUIT
Fonte: ADAPTADO DE GUO (2012)

A comunicação do *smart card* com *host* utiliza um protocolo serial *half duplex* a 9600 bps. Sua memória é limitada tipicamente entre 2 a 4 Kb.

Segundo Matos (2003), observe-se na figura 21, que atualmente a tecnologia *smart card* pode ser por:

- Contato – Neste modelo é necessário contato físico do *smart card* com a leitora, para que a mesma se comunique com o chip que está em sua superfície;
- Sem contato – Neste modelo apenas é necessário aproximar o *smart card* da leitora, pois tanto o *smart card* e o leitor possuem antenas, pelo qual se comunicam através de sinal eletromagnético;
- *Hybrid* – Neste modelo o *smart card* possui dois chips: um por contato e o outro sem contato, ou seja, o mesmo tem a opção de se comunicar por leitor de contato físico ou por leitor de proximidade;
- *Combi* – Neste modelo o *smart card* possui apenas um chip. Sendo assim, o mesmo tem a possibilidade de se comunicar por leitor de contato físico ou por leitor de proximidade.

Figura 21 – TYPES OF SMART CARD
Fonte: REVISTAGETHOME (2017)

Conforme NEDJAH, et al., (2017), o chip que é anexado ao *smart card* pode ser:

- Chip com microprocessador – Neste modelo de *smart card* pode-se ter processadores de 8, 16 ou 32bits, os quais podem realizar várias funções, tais como: adicionar,

apagar e manipular informações em sua memória, etc. Este chip é destinado para aplicações de uso de segurança alto;

- Chip de memória – Neste modelo o *smart card* funciona apenas como um local que pode armazenar informação com opcional de segurança. Portanto, a segurança do mesmo depende do leitor para processá-la. Este tipo de *smart card* é destinado para aplicações de uso de segurança baixo ou médio.

Para se utilizar o *smart card* logicamente é necessário uma leitora ou um terminal, para ler e escrever no mesmo. Existem vários tipos de leitores que se diferenciam conforme a *interface* com o PC (porta USB, *slot* PCMCIA, porta serial RS-232, porta infravermelho *IRDA*, entrada de teclado e até mesmo por *slot* de disco), sua capacidade de armazenamento e processamento (MATOS, 2003).

Segue abaixo, conforme a figura 22, um exemplo de leitora de *smart card* .

Figura 22 – LEITORA DE SMART CARD (CONEXÃO PELA PORTA USB)
Fonte: CIS (2018)

O *smart card* garante um armazenamento inviolável das chaves (pública e privada) e informações pessoais, pois ele isola o cálculo crítico de segurança relativo à troca de chaves, a autenticação e a assinatura eletrônica. Sendo assim, o algoritmo, a memória, a chave criptográfica e a entrada de dados não correm nenhum perigo de roubo de dados, pois as operações e as exibições de dados executados pelo mesmo ficam isoladas do computador. Com isso, mesmo que o usuário utilize o *smart card* em um computador que esteja infectado com algum aplicativo espião (s*pyware*), sua identidade digital continua inviolada. Por isso, os certificados tipo A3 são mais seguros (RUGGIERO, et al., 2007).

No processo de emissão da NF-e é utilizado o algoritmo desafio/resposta baseado em desafios explícitos. Sendo assim, o servidor (sistema computacional) verifica no *smart card* sua

respectiva chave privada, que o usuário está utilizando, e manda um desafio solicitando o PIN do mesmo para concluir a assinatura digital do arquivo XML da NF-e.

2.3.2.1 Java card

Durante reuniões para padronização de métodos de pagamento eletrônico na Europa, surgiu a ideia da aplicação de um cartão de aplicações múltiplas. A partir destas requisições, o pesquisador Jong (2015), desenvolveu o sistema operacional OSCAR, o qual se tornou referência para *smart card*. Em 1993 Jong patenteou o primeiro *smart card* com firewall interno pela empresa. Já em 1996 ele trabalhou em conjunto da empresa Sun com Schlumberger e desenvolveram o primeiro *java card* 1.0. Depois a empresa Visa patrocinou o projeto, para que o *java card* se tornasse um padrão em referência de arquitetura (RIBEIRO, 2015).

Em 2009 a empresa Oracle, adquiriu a Sun Microsystems e fortaleceu sua estratégia na área, dando continuidade a novas versões de linguagem de programação *java* (OLIVEIRA, 2015). A versão mais nova da tecnologia *java card* é a 3.0.5, segundo a Oracle (2018).

Segundo Chen (2000), *java card* é uma das principais linguagens utilizadas em dispositivos de segurança, com baixa capacidade de *hardware*, nos critérios de processamento, memória e também de armazenamento, executadas em particular, aplicações dentro *smart card*. O *java card* proporciona uma versão restrita da plataforma *java*, devido a limitação do *smart card*, podendo-se se beneficiar de toda a caraterística de desenvolvimento orientado a objetos, possibilitando maior interação e facilidade durante o ciclo de desenvolvimento, com utilização de bibliotecas já desenvolvidas pela própria empresa da Sun, demais comunidades e fóruns.

Segunda Oracle (2018), existem algumas limitações para a utilização do *java card*, dependendo da sua versão, de acordo com a tabela 5.

Tabela 5 – FUNCIONALIDADES SUPORTADAS E NÃO SUPORTADAS

Funcionalidades suportadas	Funcionalidades não suportadas
Tipos primitivos: boolean, byte, short	Tipos primitivos: long, double, float
Suporte ao tipo int é opcional	Caracteres e string
Arrays unidimensionais	Arrays multidimensionais
Pacotes, classes, interfaces e exceções	Threads
Herança	Clone de objetos

Fonte: DOLCE, ET AL., (2013)

A plataforma *java card* é composta por 3 partes: *Java Card Runtime Environment* (JCRE), *Java Card Virtual Machine* (JCVM) e *java card* API, conforme figura 23:

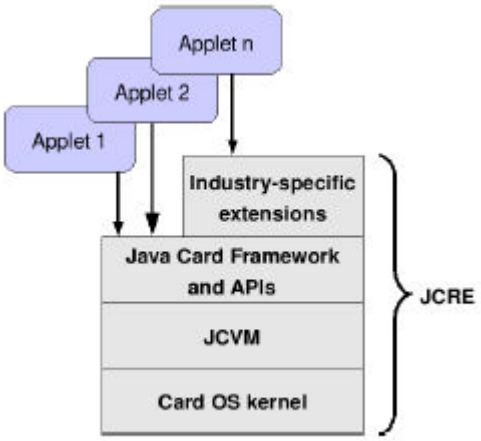


Figura 23 – COMPONENTES DA PLATAFORMA JAVA CARD
Fonte: GOMES (2012)

O JCRE é o sistema operacional do *java card*, responsável pelo gerenciamento da aplicação, onde controla-se recursos do *hardware*, comunicação e segurança. O JCRE é incorporado ao *java card*, no momento de sua fabricação. O JCRE se mantém no estado de execução durante a energização do cartão pela leitora. Uma vez suspenso, seu estado, objetos e dados ficam armazenados em memória. Quando é reiniciado, retorna o seu funcionamento de onde tinha parado, aguardando comando da aplicação do host (DOLCE, et al., 2013).

O JCVM é uma máquina virtual que está contida dentro do cartão, para que as aplicações possam serem executadas dentro ou fora deste. Devido a limitação do *hardware* no cartão se faz necessário, que os arquivos CAP (*Converted Applet*) sejam executados dentro do cartão e a conversão dos arquivos de classe em arquivos CAP sejam executados fora deste (CHEN, 2000).

Já as API's são bibliotecas e classes fornecidas pelo fabricante do cartão, para que o desenvolvedor possa criar as aplicações (ROSA JUNIOR, 2015).

2.3.2.1.1 Comunicação do java card

Como descrito anteriormente, para que haja comunicação entre o *smart card* e a aplicação, deverá existir um leitor de *smart card* (com contato ou sem contato), que fornecerá

energia para o chip interno e também funcionará como um meio físico de comunicação de dados, com transmissão em caracteres ou em blocos, segundo norma ISO 7816-3 (2016).

O padrão adotado pela plataforma de comunicação *java card* ou qualquer outro tipo *smart card* é uma arquitetura cliente-servidor, onde a aplicação cliente será denominada de host e a aplicação servidor será chamada de *applet*. O *applet* fica instalado dentro do *java card* aguardando instruções da aplicação host, que fica instalada dentro de um computador (GUO, 2012).

Para que o *applet* e o host se interajam, foi adotado pela ISO 7816-4 (2016), o protocolo de comunicação chamado de APDU (*Application Protocol Data Unit*), o qual tem a finalidade de prover serviços de:

- Comando APDU – O host solicita um serviço ao *applet* e o mesmo posteriormente processa a requisição;
- Resposta APDU – O *applet* fornece o resultado do processamento da requisição para o host.

A figura 24, demonstra a estrutura do comando APDU, onde por padrão, de acordo com a ISO 7816-4 (2016), tem que conter o cabeçalho obrigatório com quatro campos de 1 byte. Descreve-se abaixo a função de cada campo:

Cabeçalho obrigatório				Corpo opcional		
CLA	INS	P1	P2	Lc	Data field	Le

Figura 24 – ESTRUTURA DO COMANDO APDU
Fonte: DOLCE, ET AL., (2013)

- O campo CLA especifica o tipo de classe de instrução;
- No campo INS especifica o código da instrução que o *smart card* irá executar;
- P1 e P2 são utilizados como parâmetros, pelos quais a maneira que irá ser executado determina instrução;
- No campo opcional, temos o Lc onde se determina o número de bytes que serão enviados no campo *data field*;
- O *Data field* é o campo no qual consta as informações que serão enviadas em um *array* de dados;
- Já o campo Le é responsável por determinar o tamanho de bytes que receberá como resposta.

Na figura 25, apresenta a estrutura de resposta APDU, onde por padrão, de acordo com a ISO 7816-4 (2016), tem que conter no cabeçalho obrigatório dois campos de 1 byte. Descreve-se abaixo a função de cada campo:

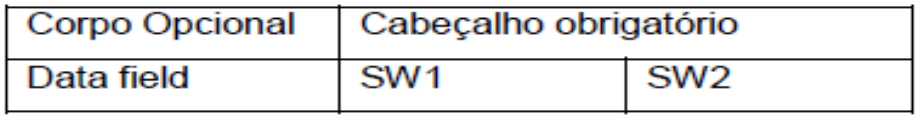


Figura 25 – ESTRUTURA DE REPOSTA APDU
Fonte: BASEADO EM GUO (2012)

- No campo opcional *Data field* é o local onde são enviados os dados de resposta da execução do comando APDU;
- Já nos campos SW1 e SW2 informa-se o status da execução do comando APDU, que é 0x90 0x00; qualquer outro código indicará que ouve falha.

Vale informar que a síntese de todos os comandos APDU são em hexadecimal, bem como, também as respostas APDU. Na tabela 6, demonstra-se alguns exemplos básicos de comandos e respostas APDU.

Tabela 6 – COMANDOS E RESPOSTAS APDU

	Comando APDU							**Resposta APDU**		
	Cabeçalho Obrigatório				Corpo Opcional			Corpo Opcional	Cabeçalho Obrigatório	
	CLA	INS	P1	P2	Lc	Data Field	Le	Data Field	SW1	SW2
1° Ex:	0x07	0x06	0x05	0x04	0x00				0x90	0x00
2° Ex:	0x07	0x06	0x05	0x04			0x01	0x0A	0x90	0x00
3° Ex:	0x07	0x06	0x05	0x04	0x03	0x02 0x02 0x02			0x90	0x00
4° Ex:	0x07	0x06	0x05	0x04	0x03	0x02 0x02 0x02	0x01	0x0A	0x90	0x00

Fonte: ADAPTADO DE SUAVI (2005)

Ainda na tabela 6, vamos descrever segundo Suavi (2005), o significado dos comandos e respostas APDU, dos quatros exemplos:

- 1° Ex: Não são enviados dados, sendo assim o Lc possui o valor 0x00 e nenhum byte como resposta é esperado;

- 2° Ex: Não são enviados dados, porém como o Le é informado. Neste caso espera-se que o *java card* envie para a aplicação host, como resposta, uma quantidade de bytes igual ao Le;
- 3° Ex: Agora o Lc informa o número de bytes que será enviado ao *smart card*, ou seja, o tamanho dos dados enviados no campo *data field*;
- 4° Ex: O Lc informa o número de bytes que será enviado ao *smart card*, só que agora se espera uma resposta do *smart card* com número de bytes igual a Le.

2.3.2.1.2 Aplicações em java card

Uma aplicação em *java card*, pode ser desenvolvido de duas maneiras, segundo Gomes (2012):

- APDU (*Application Protocol Data Unit*);
- RMI (*Remote Method Invocation*).

Aplicações em *java card*, que são desenvolvidas por APDU são mais complexas. Neste caso pode-se desenvolver código em baixo nível, onde a comunicação é feita bit a bit no *java card*, através dos comandos APDU.

Já em aplicações *java card*, que são desenvolvidas por RMI, utiliza-se a plataforma de comunicação cliente-servidor, onde o desenvolver só se preocupa em invocar métodos (RMI). Neste caso lida-se apenas com objetos das classes entre o *host* e o *applet*, onde o protocolo APDU é abstraído.

A figura 26, mostra um exemplo de fluxo padrão de uma aplicação *java card*. Em seguida descrever-se as etapas de criação, instalação e execução de um *applet* dentro do mesmo, segundo DOLCE, et al., (2013):

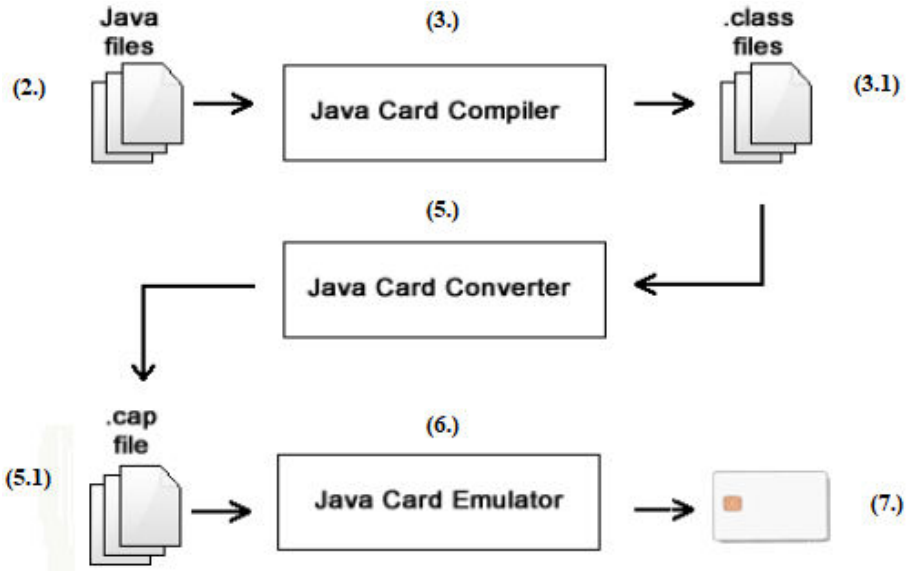


Figura 26 – ETAPAS DE DESENVOLVIMENTO

Fonte: DOLCE, ET AL., (2013)

1. Seguem o padrão da norma ISO 7816-4 (2016). Os comandos APDU e sua resposta são executados dentro do *java card*: comandos de inserir, consultar e excluir dados;
2. Baseado na arquitetura cliente-servidor, é necessário criar a aplicação servidor que é nosso *applet* em código *java*, o qual é responsável de prover serviços para a aplicação cliente (*host*), bem como, classes auxiliares que serão utilizadas pelo *applet*;
3. Após a criação do *applet* e demais classes auxiliares, através da compilação feita pelo *java card compiler*, são gerados os arquivos *.class (3.1);
4. Dentro do *java card* pode haver um ou vários *applets*, sendo assim, cada applet possui um número de identificação chamado de AID (*Applet Identification*). A aplicação host quando vai solicitar algum dado ao *java card*, deve primeiro informar através de um comando de seleção, o AID do *applet* que irá prover a informação que se deseja consultar;
5. Na etapa do *java card converter*, todos os arquivos * .class devem ser convertidos em um único arquivo cap (5.1), e é também setado o AID do *applet*;
6. Agora em um de ambiente de desenvolvimento é possível instalar o arquivo *.cap, dentro do *java card emulator*, ou até mesmo dentro do *java card* físico;
7. Com a aplicação servidor (*applet*) já está instalada no *java card*, agora é possível, através da aplicação cliente (*host*), enviar-se comandos APDU e também obter-se respostas APDU.

De acordo com as etapas acima, toda vez que o *applet* é convertido, executa-se uma verificação de síntese do código, em conformidade com as especificações do *java card*, antes do mesmo ser instalado dentro do *smart card*.

Segue-se alguns métodos básicos de relacionamento de herança da classe principal *applet* (javacard.framework.Applet) (BLOKDYK, 2018):

- O método *install* é chamado pelo JCRE apenas na primeira vez em que o *applet* é executado, ou seja, é o primeiro a ser acessado dentro do *applet* com a responsabilidade de criar uma instância da classe *applet* e registrá-la junto ao ambiente de execução. Como apenas uma instância do *applet* é registrada por vez, o JCRE tem a reponsabilidade de responsável por gerenciar a mesma;
- Já o método *process* é quem recebe o comando APDU e verifica sua síntese, o qual se estiver válida, direciona para a aplicação servidor e executar o mesmo.
- Com o método *Select* permite-se selecionar o AID do *applet*, e retorna-se um valor *true* caso a aplicação seja selecionada;
- No método *deSelect* pode-se retirar a seleção da aplicação e deixar o *smart card* liberado para utilizar outro *applet*.

2.4 BIOMETRIA

Segundo Thing (2003), define-se que biometria (do grego bio=vida e métron=medida) é a ciência e a tecnologia que mede e analisa estaticamente dados biológicos. Já para área de informática o estudo da biometria se concentra cada vez mais em desenvolver formas de capturar características comportamentais, ou do corpo humano, e transformá-las de forma digital. Posteriormente, utilizar tais características, já em sua forma digital, em aplicações de sistemas de controle de autenticação, onde seus usuários previamente cadastrados, podem realizar ou não determinadas ações e serviços.

Observando a história das antigas civilizações, percebe-se que as mesmas já se beneficiavam da biometria, como é o caso da dinastia Tang (618-907 d.C.) que grafava em placas de barro as impressões digitais para identificação posterior dos indivíduos em transações comerciais. Este foi o primeiro fato histórico no qual foi utilizada a impressão digital de forma eficaz. O italiano Marcello Malpighi (1628-1694) na Universidade de Bolonha foi um dos primeiros a estudar as linhas em relevo nas pontas dos dedos, as quais se chamam de cristas. Já

o francês Alphonse Bertillon, no final do século XIX, desenvolveu em seus estudos um método antropométrico ou *bertillonage* aprovado oficialmente, que combinava as medidas físicas coletadas e as documentavas para identificação posterior de seus indivíduos (PINHEIRO, 2008).

Hoje em dia, para que um sistema biométrico seja seguro, segundo Pinheiro (2008), é necessário que o mesmo atenda aos requisitos abaixo:

- O sistema tem que ser seguro e robusto contra técnicas de fraudes;
- As características observadas do indivíduo têm que ser estáveis durante o percurso de sua vida;
- Devem existir características biométricas diferentes para cada indivíduo (singularidade), ou seja, caso exista duas pessoas com a mesma característica biométrica, que está probabilidade seja muito pequena;
- É necessária a opção de quantitativamente poder ser medida (mensurabilidade), com base no modelo da característica selecionada;
- O sistema deve haver certo nível de aceitação pelos usuários em relação ao reconhecimento biométrico;
- O sistema deve possuir um bom desempenho durante a aquisição e comparação biométrica de cada indivíduo;
- Um fator importantíssimo que o sistema tem que ter é uma precisão de reconhecimento biométrico aceitável.

A figura 27 apresenta o esquemático de um processo básico de um sistema biométrico (PEREIRA, 2016):

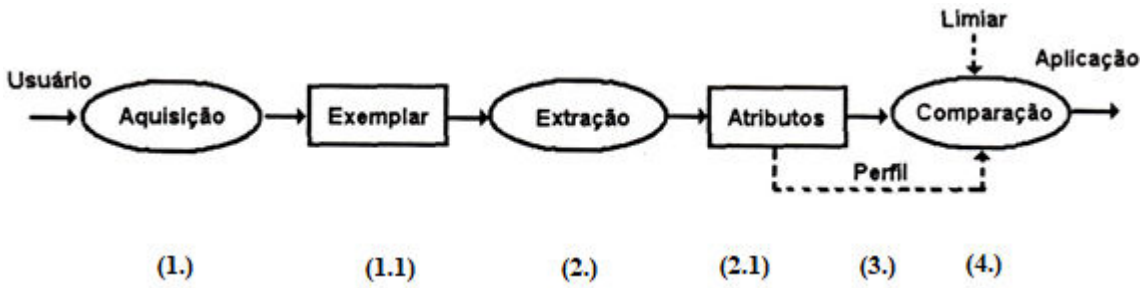


Figura 27 – PROCESSO BÁSICO DO SISTEMA BIOMÉTRICO

Fonte: PINHEIRO (2008, pág. 44)

O processo pode ser assim descrito:

1. Aquisição e exemplar (1.1) – Nesta primeira etapa é capturada a característica biométrica do indivíduo através de dispositivos ou sensores, que utiliza um *software* capaz de converter a amostra biométrica em um modelo digital. A informação capturada nesta etapa é em um banco de dados para posterior comparação. Vale informar que uma boa qualidade da amostra feita pelo sensor ou dispositivo, ajudará muito no desempenho do sistema biométrico;
2. Extração e atributos (2.1) – A etapa de extração é uma representação do exemplar capturada, de forma digital, denominado de atributo ou *template*;
3. Perfil e registro – Nesta etapa é efetuado o primeiro registro do usuário, o qual é efetivado apenas uma vez. Sendo assim, durante este registro é cadastrado toda informação biométrica em um perfil, ou seja, em um *template*, associado com um identificador do usuário, que será utilizado para posteriores comparações;
4. Comparação, limiar e decisão – Nesta etapa final é feito uma comparação de semelhança entre a amostra biométrica capturada pelo indivíduo, com o perfil que foi armazenado anteriormente, o *template*. Caso o limiar, limite superior de similaridade, esteja a certo padrão de aceitação, o sistema identifica o indivíduo em quem diz ser e libera o seu acesso para posteriores aplicações. Caso contrário, é negado imediatamente o seu acesso.

Segundo Pinheiro (2008), a arquitetura de um sistema básico de biometria é composta por em quatro componentes:

1. Subsistema interface de usuário (sensor biométrico) – Este subsistema utiliza um sensor ou dispositivo para capturar característica física do indivíduo, onde posteriormente o converte em um padrão adequado para ser mandada para o subsistema de estação de controle;
2. Subsistema estação de controle (cérebro) – Este subsistema é responsável por controlar todas as funções do dispositivo, desde os recursos de processamento, armazenamento da informação, até sua programação. Ao receber do subsistema interface de usuário a amostra biométrica do indivíduo, o subsistema estação de controle a converte em um padrão adequado para ser mandado para o subsistema comparador;
3. Subsistema comparador (comunicações e processamento) – Este subsistema é responsável por comparar a similaridade (limiar) da amostra biométrica apresentada pelo indivíduo com o *template* armazenado anteriormente pelo subsistema de

armazenamento. Portanto, o subsistema comparador também interage na comunicação com outras partes do sistema, para auxiliar e enviar resultados;

4. Subsistema de armazenamento (banco de dados) – Este subsistema é responsável por armazenar em *token* em *hardware*, *smart card*, banco de dados centralizado, entre outros, todos os *templates* dos indivíduos. Por isso, este subsistema de armazenamento, além de poder efetuar as funções de subtração, adição ou atualização do *template* para os dispositivos de armazenamento, pode, dependendo da aplicação do sistema, associar um *template* ou vários para cada indivíduo.

A figura 28, apresenta o fluxo de etapas descritas anteriormente, desde o registro até a etapa de verificação.

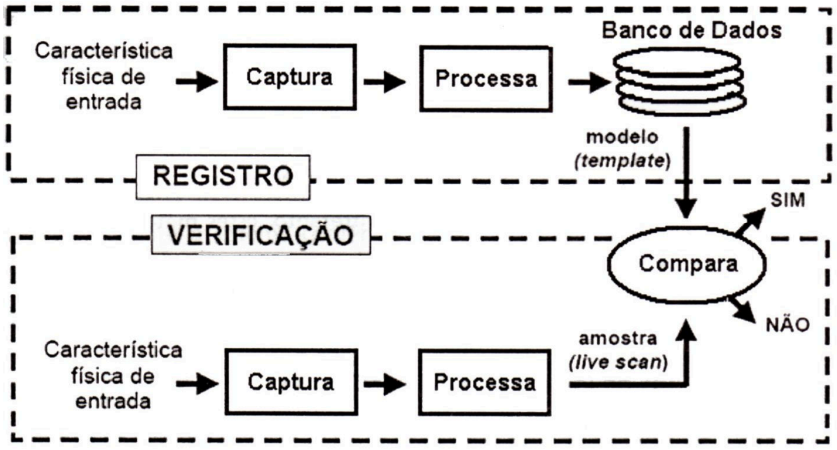


Figura 28 – MODELO DE REGISTRO E VERIFICAÇÃO DE UM SISTEMA BÁSICO DE BIOMETRIA
Fonte: PINHEIRO (2008, pág. 55)

Segundo Nunes (2015), os tipos de elementos pelos quais os sistemas biométricos se baseiam está nas características do indivíduo: Anatômicas (física) ou comportamental, conforme figura 29.

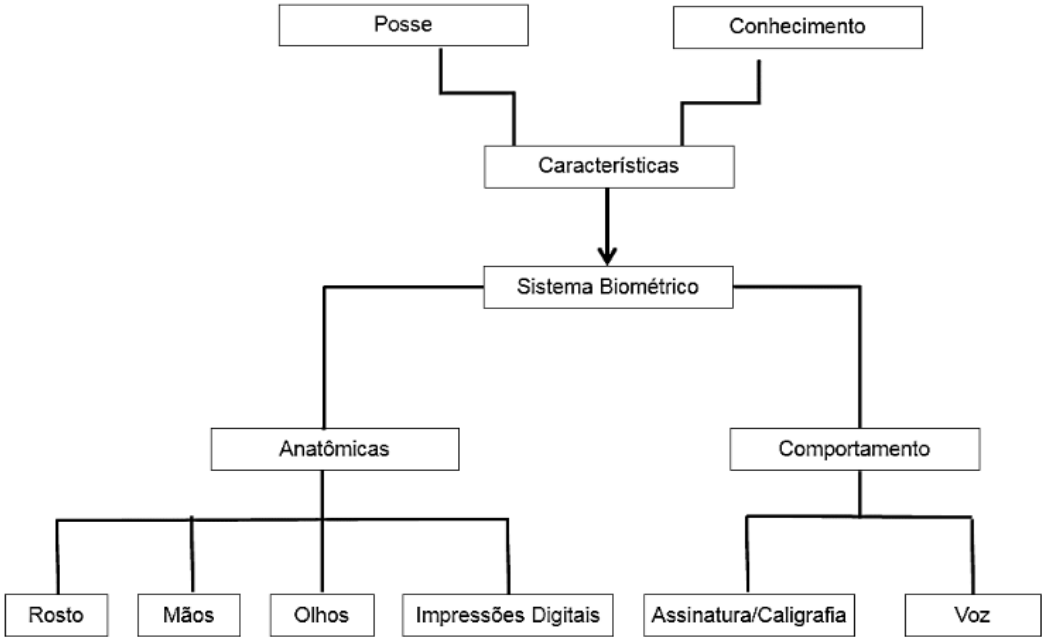


Figura 29 – TIPOS DE ELEMENTOS BIOMÉTRICOS

Fonte: NUNES (2015)

Serão demonstrados nos seguintes tópicos abaixo, apenas os principais e mais utilizados sistemas de reconhecimento biométrico.

2.4.1 Impressão digital

O sistema biométrico por reconhecimento da impressão digital aborda uma característica física do indivíduo, a saber: análise das minúcias de cada um de seus dedos (FERREIRA, 2015).

Este sistema é um dos mais estudados e utilizados atualmente desde o século XIX, por sua implementação ser de baixo custo e de boa aceitação pelos usuários. Sendo assim, em 2011 os dispositivos biométricos por impressão digital contabilizaram 50% das vendas em relação aos produtos do mesmo gênero (CAMPOS, 2007).

A impressão digital de cada indivíduo é única, com isso, o sistema por reconhecimento de impressão digital tem um nível de segurança médio, pois durante o ciclo de vida do usuário as características das digitais dos dedos são pouco prováveis de mudar. Portanto, o mesmo só fica atrás dos sistemas de reconhecimento por DNA, retina, íris e mapas de veias (ALEJO, 2015).

A impressão digital de cada indivíduo é formada por vários sulcos, que apresentam diferenças, e que são chamadas de pontos de minúcias. Existem dois tipos de minúcias os quais

são mais utilizadas para o processo de extração e comparação dentro de um sistema por reconhecimento de impressão digital: pode-se observar o exemplo de crista de terminações e a de bifurcações (NEDJAH, et al., 2017). Na figura 30 tem uma impressão digital, na qual se pode verificar a crista de terminações e de bifurcações.

Figura 30 – FINGERPRINT AND MINUTIAE
Fonte: NEDJAH, ET AL., (2017)

Segundo Campos (2007), a captura da impressão digital de um indivíduo pode ser feita atualmente através de três tipos de dispositivos, que se diferenciam através do seu tipo de *scanner*:

- Capacitivo – Este dispositivo trabalha medindo o calor que sai da digital do dedo do indivíduo;
- Ótico – Este dispositivo é o mais utilizado, pois em seu funcionamento ao colocar o dedo do usuário no vidro do dispositivo, o mesmo faz uma varredura (*scanner*) emitindo uma luz sobre a digital. Através do fenômeno da reflexão da luz emitida, o dispositivo consegue capturar as informações das minúcias. Vale informar que mesmo que o dedo do usuário esteja sujo, o dispositivo ainda é capaz de capturar com sucesso as informações das minúcias, tornando assim o dispositivo de reconhecimento de impressão digital mais seguro;
- Ultrassônico – Este dispositivo trabalha como se fosse um dispositivo ótico, com apenas uma diferença. Ao invés de emitir uma luz, o mesmo emite sinais sonoros para analisar o retorno deles, capturando assim as informações das minúcias.

Porém, apenas ter um bom *scanner* não é suficiente, pois é essencial ter um bom *software* para dar um tratamento na imagem capturada. Esta imagem capturada possui em geral de 256 a 669 bytes.

Uma vez capturada, estas imagens são válidas através de um dos seguintes processos (PINHEIRO, 2008):

- Sistema de impressão latente – Neste sistema, após a captura da imagem está é comparada com as impressões digitais existentes em um banco de dados central, a fim de determinar de quem é esta impressão digital. Vale lembrar que comparação de impressões digitais feitas em um banco de dados central, torna a resposta da aplicação mais lenta;
- Sistema real time – Em tempo real, após a captura da impressão digital, a mesma é processada e comparada com outras impressões digitais, armazenadas em seu banco de dados local, o que a torna mais rápida.

Para obter uma boa captura das impressões digitais do indivíduo no primeiro registro (perfil) são necessários que os dedos não estejam com as minúcias úmidas, muito secas, sujas ou desgastadas, pois durante o processo são capturadas as digitais de todos os dedos das mãos, para formar um arquivo decadáctila (PINHEIRO, 2008).

Posteriormente, se o indivíduo precisar ser identificado por alguma aplicação de sistema biométrico por impressão digital, onde desde um dos seus dedos estiver com a impressão digital danificada, não tem nenhum problema, desde que as outras impressões digitais do indivíduo poderão identificá-lo. Este fato acontece com frequência com pessoas que trabalha em lavanderia, oficina e entre outros.

2.4.1.1 Método biométrico finger scan

O método biométrico *finger scan* é o modelo padrão para os dispositivos de captura das minucias de um indivíduo, já que o método coletado via tinta e inserido no papel, não está sendo mais utilizado atualmente.

A figura 31 apresenta alguns tipos de minucias que são coletados durante a captura da impressão digital.

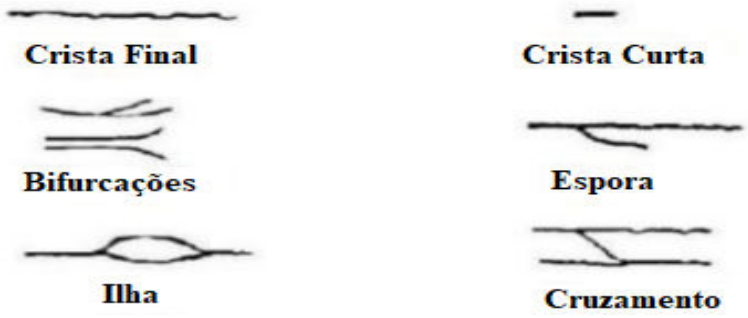


Figura 31 – ALGUNS TIPOS DE MINÚCIAS
Fonte: RICARDO (2012)

Pode-se abordar um algoritmo de extração de minúcias clássico segundo Oliveira, et al., (2016), o qual define 2 módulos básicos: Um de pré-processamento e outro de pós-processamento, como pode ser visto na figura 32.

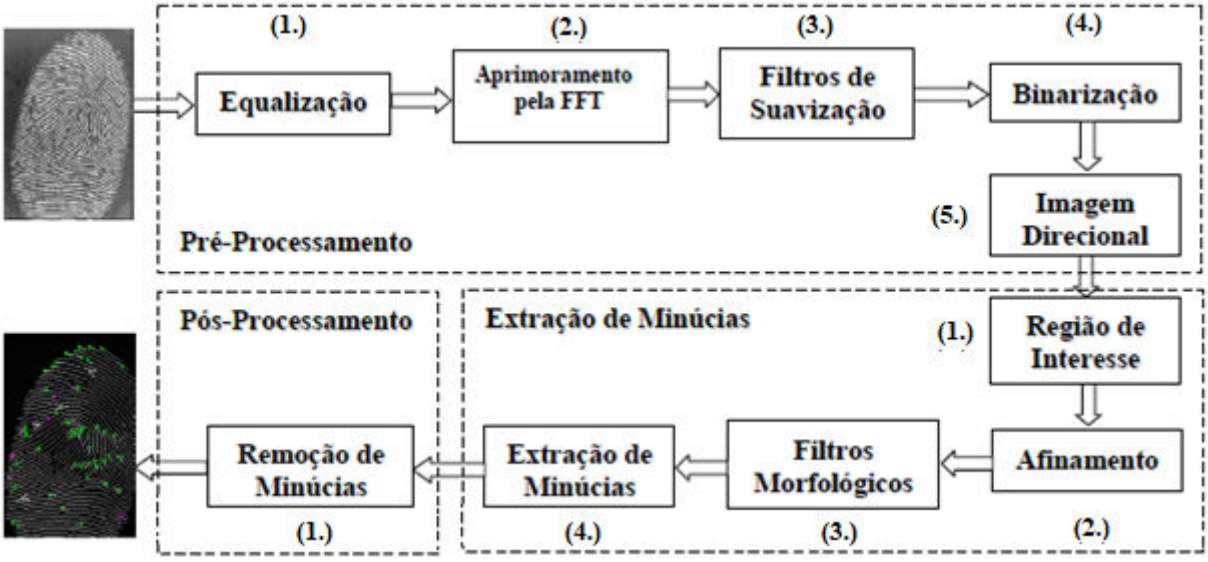


Figura 32 – MÓDULOS DO ALGORITMO DE EXTRAÇÃO DE MINÚCIAS
Fonte: CASADO (2008)

O módulo de pré-processamento é responsável de efetuar um pré-processamento da imagem, aumentar a discriminação visual e extrair as minúcias, onde o mesmo se divide em cinco etapas abaixo (CASADO, 2008):

1. Equalização – Nesta etapa inicial é realizado o espalhamento de contraste da imagem, para melhorar a qualidade da mesma, evitando assim a captura de pixels similares, que acabam criando falsas minúcias. Esta técnica consiste em calcular um valor médio de intensidade de vizinhos em um bloco de 5x5, para posteriormente determinar um valor para cada *pixel*. Se a intensidade de unidade *pixel* for menor que

a média do bloco, então este recebe o valor zero, se não, o *pixel* continua com seu valor inicial;

2. Aprimoramento pela FFT (*Fast Fourier Transform*) – Agora é aplicado um aprimoramento na imagem, em cada bloco de processamento de 32x32 *pixels*, através da equação de transformada de Fourier:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) * \exp\left\{-j2\pi * \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\}$$

Para u = 0, 1, 2,..., 31 e v = 0, 1, 2,..., 31

Este procedimento permite que cada crista final ou curta, que foi prejudicada por algum distúrbio, possa se conectar novamente, evitando-se que as cristas se unam umas com as outras, ou seja, não haja uma bifurcação;

3. Filtros de suavização – Deve-se agora aplicar na imagem, um filtro da média para suavizar as bordas das cristas papilares e atenuar o distúrbio existentes entre o espaço das cristas, chamados de vales, e em seguida aplicar um filtro gaussiano passa-baixa, para atenuar o efeito dos blocos de *pixels* da etapa anterior;
4. Binarização – Após a etapa anterior, chegou a hora de transformar a imagem original de 8 bits/pixel em uma de 1 bit/pixel, atribuindo o valor 1 para as cristas papilares e o valor 0 para os vales. Esta etapa é responsável por transformar a imagem da impressão digital em tons de cinza, para uma em preto e branco;
5. Imagem direcional – Na etapa final do módulo de pré-processamento a imagem é classificada dentro de um dos cinco padrões adotados pelo NIST (*National Institute of Standards and Technology*): Verticilo, arco plano, presilha externa e presilha interna. Esta classificação agiliza o processo de reconhecimento do indivíduo, bem como, utilizada no módulo de pós-processamento, ajuda a remover falsas minúcias.

Na etapa do módulo de extração de minúcias, remove-se falsas minúcias, através de quatro etapas, como descrito abaixo (CASADO, 2008):

1. Região de interesse – O algoritmo utilizado inicialmente na etapa de extração de minúcias é responsável por determinar a região de interesse que contém as informações importantes da impressão digital. Este algoritmo utiliza os operadores morfológicos *opening* e *closing*;

2. Afinamento – Agora é aplicado um afinamento da imagem. Este algoritmo deve compactar dados, eliminar ruídos sem introduzir deformidades, bem como, deve manter as caraterísticas significativas dos padrões;
3. Filtros morfológicos – Depois da etapa anterior, é aplicado na imagem, outra sequência de filtros: clean, hbreak e spur, onde removem alguns pixels errôneos;
4. Extração de minúcias – O algoritmo consiste em aplicar na imagem linha a linha, uma máscara 3 x 3 para detectar bifurcações e outra para detectar terminações.

Por fim, o módulo de pós-processamento executa apenas uma etapa, descrito abaixo (CASADO, 2008):

1. Remoção de minúcias – Nesta etapa final, é aplicado novamente um algoritmo de remoção de falsas minúcias, os quais não foram eliminadas nas etapas anteriores. Este processo é muito importante, pois vai definir a qualidade final da captura da impressão digital.

Descreve-se abaixo, seis etapas do método de comparação das minúcias, o qual este método é confiável, rápido e com baixo custo de implementação, conforme figura 33:

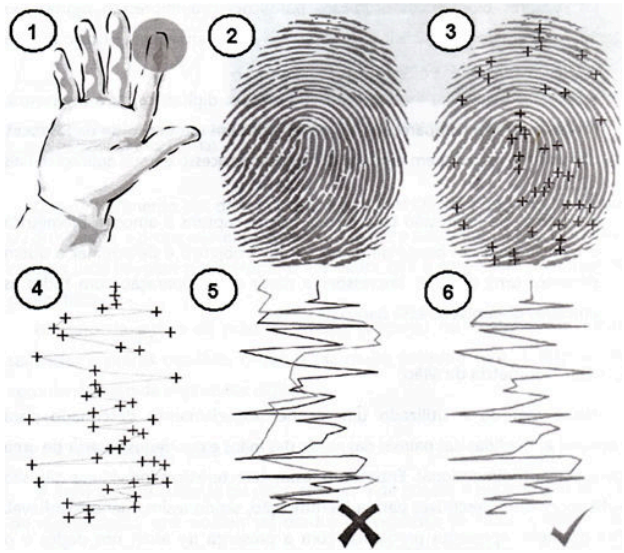


Figura 33 – MÉTODO DE COMPARAÇÃO DAS MINÚCIAS
Fonte: PINHEIRO (2008, pág. 65)

1. Seleção da fonte da amostra;
2. Captura da impressão digital;
3. Mapeamento das minúcias;

4. Geração do modelo a partir do algoritmo;
5. Comparação no banco de dados;
6. Identificação positiva.

Dependendo do fabricante do leitor biométrico, alguns já fornecem um sistema embarcado de captura das minúcias e de processamento de imagem dentro do dispositivo, bem como, *drivers* de comunicação com o sistema operacional e uma biblioteca (DLL). Isto é bastante útil, pois abstrai a camada de *hardware*, fazendo com que o desenvolver só se preocupe de utilizar os métodos determinados pelo fabricante.

Observe-se abaixo a definição do que é uma DLL, de acordo com um fabricante de leitor biométrico:

> Uma DLL é uma biblioteca de vínculo dinâmico que contém código e dados que podem ser usados por mais de um programa ao mesmo tempo. Ao usar uma DLL, um programa pode ser modularizado em componentes separados, atualizações são mais fáceis de aplicar a cada módulo sem afetar outras partes do programa, são utilizados menos recursos e ajudam a promover a reutilização de código. (CIS, 2017).

Sendo assim, vamos utilizar o uso de DLL e seus métodos para o nosso processo de captura da impressão digital, assim como, a tecnologia LFD, que será utilizada em nosso leitor biométrico para captura de impressão digital.

2.4.1.2 LFD (live finger detection)

Um grande problema na eficiência de captura da impressão digital é o fato do mesmo, poder ser burlado com um dedo falso, de materiais como silicone, argila, gelatina, borracha, entre outros. Observe-se abaixo um comentário de um fabricante de leitor biométrico:

> After the release of the iPhone 5S and introduction of a built-in fingerprint sensor, contests were held to crack the device's fingerprint scanner have been held with lots of hackers joining the competitions and numerous IT magazines reported about the vulnerability of the fingerprint sensor against fake fingerprints. Numerous videos have been recently uploaded on YouTube where hackers breached the security by making fake fingerprints from Play-Doh, gelatin, silicone, rubber and the like and explained how to make the fake fingerprints. (SUPREMA, 2016).

Diante deste fato, o que foi proposto no estado da arte atualmente para solucionar tal problema?

Como uma das alternativas para solução de tal problema, foi desenvolvida a tecnologia LFD (*Live Finger Detection*), capaz de evitar o chamado *spoofing*, ou seja, autenticação com impressões digitais falsas.

A tecnologia LFD é baseada na análise das características dinâmicas e estáticas da imagem dos dedos, ou seja, das minúcias. Cada fabricante de leitor biométrico por impressão digital, adota seu próprio algoritmo de análise avançada para detectar anormalidades no padrão de mudança dinâmica de imagem da impressão digital. Estes tipos de algoritmos são propriedades patenteadas de cada fabricante. A função deste algoritmo de análise avançada verifica também características estáticas de vivacidade ou não naturalidade dos dedos, com isso os dedos falsos são claramente diferenciados dos dedos vivos. Esta técnica é associada a outras de aferição da pressão arterial, temperatura, pulso, resistência elétrica, sensor de proximidade e a pressão exercida do dedo em cima no vidro do scanner de captura das minúcias (SOUSEDIK, et al., 2013).

Um algoritmo de análise avançada *adaptive gain control*, adotado e divulgado pela empresa Suprema (2016), em relação à:

- Análise dinâmica de padrões de mudança;
- Análise de recurso de vivacidade;
- Análise de características não naturais;
- LDE (*Liveness Decision Engine*).

Análise dinâmica de padrões de mudança – Este tipo de análise verifica de forma contínua as imagens das impressões digitais e seus padrões de mudança, conforme na figura 34. Isto permite a detecção de impressões digitais falsas feitas por materiais duros como borracha, filme, argila e papel, não é característica de um dedo vivo, que tem a característica de demonstrar mudanças nos padrões de área, intensidade e movimento, à media que o mesmo gradualmente entra em contato com a superfície de vidro do sensor biométrico.

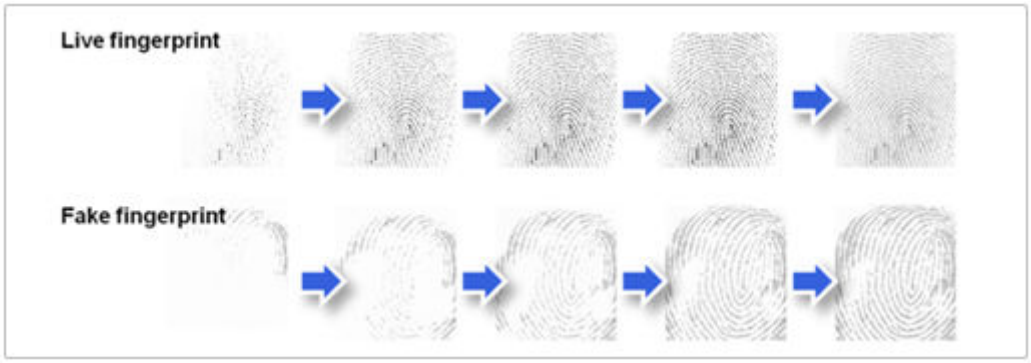


Figura 34 – DYNAMIC CHANGING PATTERN ANALYSIS
Fonte: SUPREMA (2016)

Análise de recurso de vivacidade – Com um bom sensor de captura de minúcias é possível identificar a vivacidade de um dedo vivo: características localizadas muito pequenas de agudeza, distribuição dos poros, regularidade do limite entre os cumes e entre outros. Um dedo falso feito de material simples e suaves, como gelatina, borracha e silicone, não consegue reproduzir tais características. O algoritmo de análise avançada consegue distinguir tais discrepâncias, como pode ser visto na figura 35.

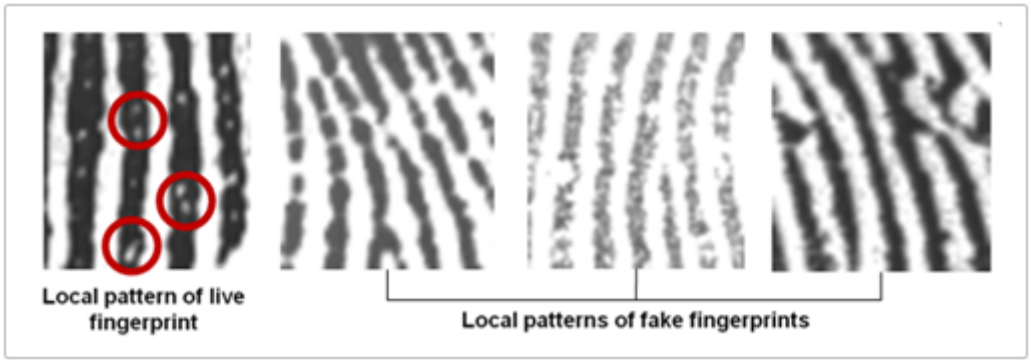


Figura 35 – LIVENESS FEATURE ANALYSIS
Fonte: SUPREMA (2016)

Análise de características não naturais – Neste método de análise avançado, é verificada a mistura de numerosas características antinaturais, conforme na figura 36, como: limites nítidos não naturais, grandes manchas pretas na área da impressão digital ou muitas bolhas brancas, picos anormais na distribuição do histograma e assim por diante. Mais um recurso que faz com que o algoritmo consiga detectar um dedo falso com facilidade.

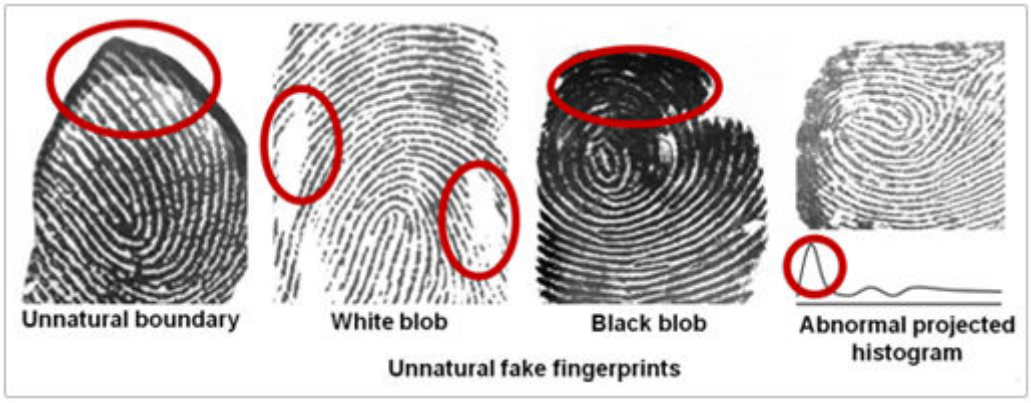


Figura 36 – UNNATURALNESS FEATURE ANALYSIS
Fonte: SUPREMA (2016)

LDE (*Liveness Decision Engine*) – Com o avanço da tecnologia LFD, foi incorporado a mesma a tecnologia *dual light source imaging*, que tem a função de incidir sobre o dedo raios infravermelhos e uma luz branca, conforme na figura 37, comparando imagens obtidas e com isso evitando o *spoofing*. Este tipo de tecnologia consegue facilmente bloquear autenticações de impressões digitais falsas feitas de silicone, cola, papel, filme, borracha e argila.

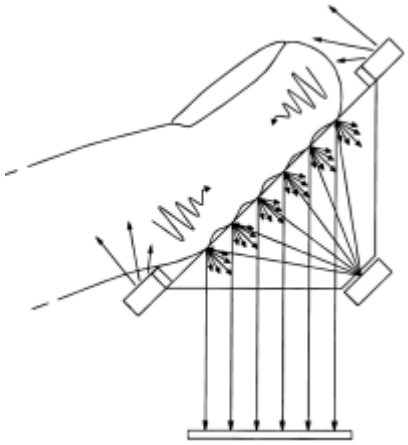


Figura 37 – LIVENESS DECISION ENGINE
Fonte: SUPREMA (2016)

Diante destes fatos, para se evitar autenticação com impressão digital falsa (*spoofing*), é que neste projeto, foi adotado um leitor biométrico por captura de impressão digital, que utiliza a tecnologia LFD. Tal tecnologia não só empresa Suprema utiliza, como por concorrentes. A diferença de desempenho entre elas está na eficiência do algoritmo de análise avançada adotado por cada uma.

2.4.2 Reconhecimento pela retina

O sistema biométrico por reconhecimento pela retina se concentra em analisar a característica física do globo ocular, em específico, a camada dos vasos sanguíneos no fundo dos olhos, chamada de retina.

Para implementação de um sistema biométrico por reconhecimento pela retina, requer-se um dispositivo (leitor) capaz de emitir uma luz de infravermelho de baixa intensidade no globo ocular para se fazer a varredura da retina. Porém este tipo de sistema tem um custo elevado para seu desenvolvimento e implantação, além de também existir um inconveniente, pois o usuário tem que tirar os óculos, caso use, olhar para o visor, e focalizar em um determinado ponto da luz do infravermelho (ALEJO, 2015).

Descreve-se abaixo quatro etapas do método de comparação, dos vasos sanguíneos da retina, conforme figura 38:

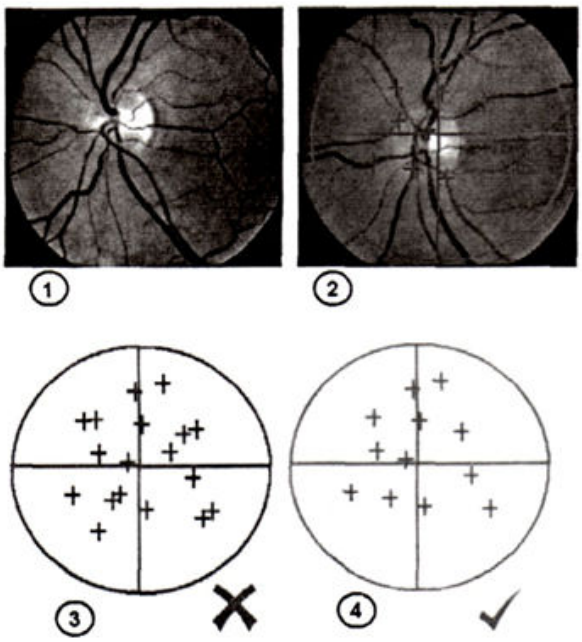


Figura 38 – MÉTODO BIOMÉTRICO DE RECONHECIMENTO PELA RETINA
Fonte: PINHEIRO (2008, pág. 71)

1. Aquisição da imagem da retina;
2. Aplicação do algoritmo e obtenção das características;
3. Comparação com o *template* armazenado no banco de dados;
4. Identificação positiva.

2.4.3 Reconhecimento facial

O sistema biométrico por reconhecimento facial se baseia na análise de algumas características físicas do rosto do indivíduo; quais sejam: a distância entre os olhos, a distância entre boca, nariz e olhos e a distância entre olhos, queixo, boca e linha dos cabelos.

Na figura 39, pode ser visualizado o mapeamento da face, em três etapas e também como é feita a identificação pelo dispositivo (leitor).

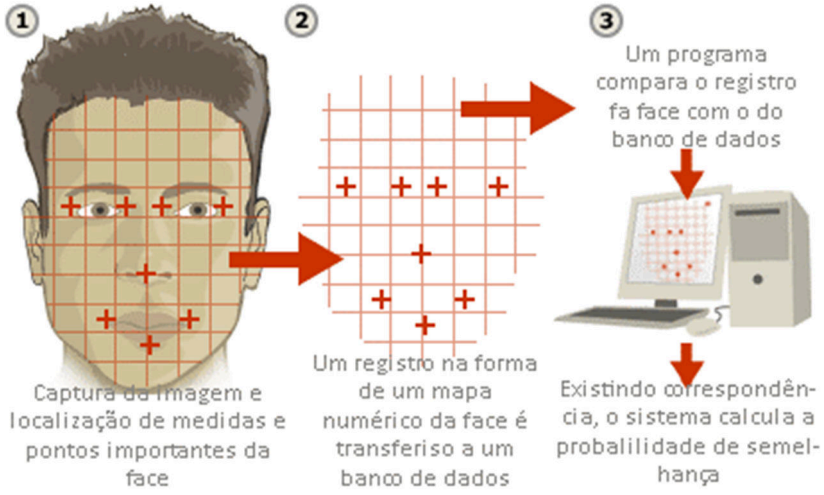


Figura 39 – MÉTODO BIOMÉTRICO DE RECONHECIMENTO FACIAL
Fonte: TECMUNDO (2011)

A tecnologia de reconhecimento facial por ser um sistema menos intrusivo é bem aceito pelos usuários, porém durante o ciclo de vida do usuário é muito provável que suas características faciais mudem, tornando assim este sistema com um nível de segurança baixo (CAMPOS, 2007).

Em alguns sistemas biométricos por reconhecimento facial mais inteligente, já é solicitado ao usuário, que ao se deparar com a câmera na hora do seu primeiro registro e posteriormente em um processo de comparação, que o mesmo dê um sorriso ou pisque os olhos. Isto impede que um intruso coloque, por exemplo, um boneco na frente da câmera para se passar pelo usuário verdadeiro. Vale ressaltar que o sistema biométrico por reconhecimento facial tem um custo elevado de implementação (ALEJO, 2015).

2.4.4 Identificação pela íris

O sistema biométrico por reconhecimento pela íris se concentra em analisar apenas a íris do usuário.

A íris é a parte colorida do olho que fica em torno da pupila, que apresenta 249 pontos, que podem ser analisados por sistemas biométricos. Cada indivíduo possui uma característica única de sua íris, o que faz com que este sistema biométrico tenha um nível de segurança muito alto, ficando atrás somente do sistema de reconhecimento por DNA. As características da íris são impossíveis de mudar durante o ciclo de vida do usuário (MELO, 2016).

Na figura 40 descreve-se as etapas do processo de identificação da íris pelo dispositivo (leitor):

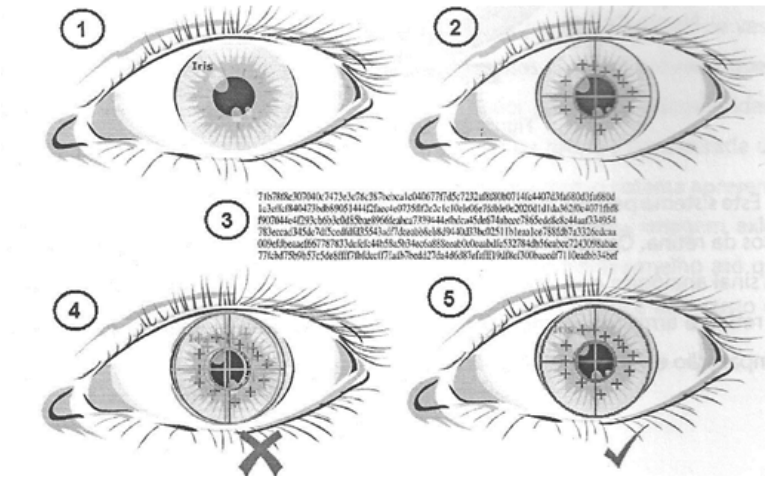


Figura 40 – MÉTODO BIOMÉTRICO DE IDENTIFICAÇÃO POR ÍRIS
Fonte: TECMUNDO (2011)

1. Imagem da íris adquirida sob condições ideais;
2. Aplicação do algoritmo e reconhecimento das características;
3. Geração do ÍrisCode associado;
4. Comparação com os padrões armazenados no banco de dados;
5. Identificação positiva.

2.4.5 Reconhecimento pela voz

O sistema biométrico por reconhecimento de voz concentra-se em analisar uma característica comportamental do indivíduo neste caso a voz.

Vale lembrar que o algoritmo do sistema biométrico por reconhecimento de voz não compara a voz do indivíduo, de fato ele faz uma análise da harmônica e analisa a probabilidade de cada fonema (PINHEIRO, 2008).

A característica da voz é pouco provável de ser mudada durante o ciclo de vida do usuário, porém existem alguns problemas que podem ocorrer com este tipo de sistema, impedindo que o usuário legitimo possa ser identificado corretamente durante a captura de sua voz; o barulho do próprio ambiente, a voz roca e até mesmo o nervosismo por parte do usuário (CAMPOS, 2007).

A figura 41 apresenta o fluxo de aquisição de voz pelo sistema de reconhecimento de voz.

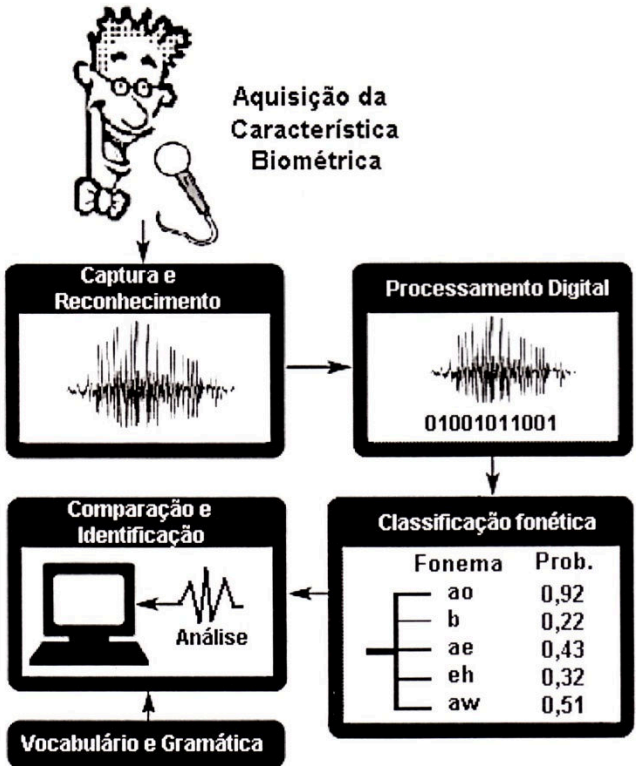


Figura 41 – RECONHECIMENTO DE VOZ

Fonte: PINHEIRO (2008, pág. 73)

2.4.6 Reconhecimento da assinatura manuscrita

O sistema biométrico por reconhecimento da assinatura manuscrita se concentra em analisar a assinatura do indivíduo.

Seu funcionamento se baseia em dois tipos:

- Sistemas *on-line* (dinâmico) – Este tipo de sistema analisa durante a assinatura do indivíduo as características do formato de cada letra, velocidade e a pressão exercida pela caneta sobre o dispositivo (leitor), os quais são enviadas para um banco de dados, onde posteriormente poderão ser usadas para comparação e verificação da identidade do indivíduo. Pode-se dizer que este sistema biométrico por reconhecimento de assinatura manuscrita é de reconhecimento dinâmico de assinaturas, conforme a figura 42;

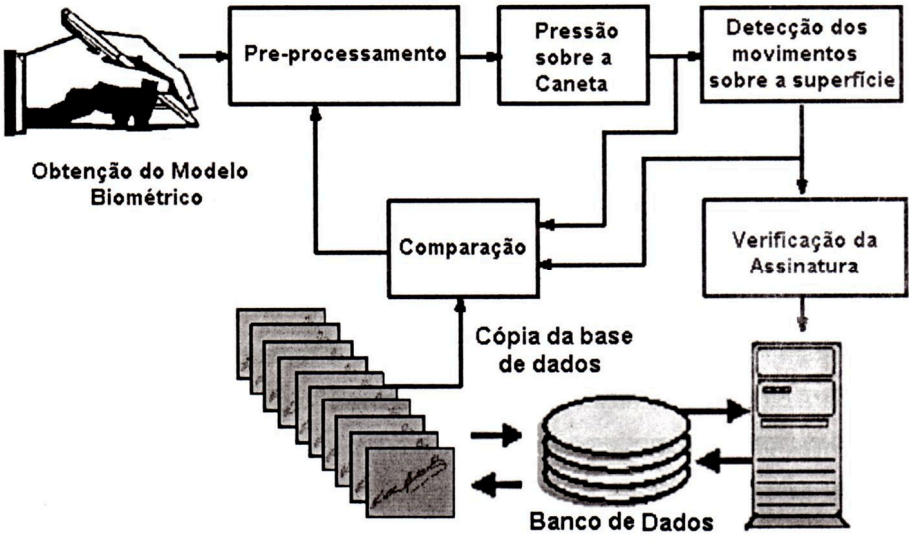


Figura 42 – RECONHECIMENTO DINÂMICO DE ASSINATURA
Fonte: PINHEIRO (2008, pág. 79)

- Sistemas *off-line* (estático) – Este tipo de sistema captura do indivíduo a imagem da sua assinatura através de um dispositivo (leitor) e a envia para um banco de dados, onde posteriormente poderá ser feito comparação e verificação da identidade do indivíduo. Pode-se dizer que este sistema biométrico por reconhecimento da assinatura manuscrita é de reconhecimento estático de assinaturas, conforme a figura 43.

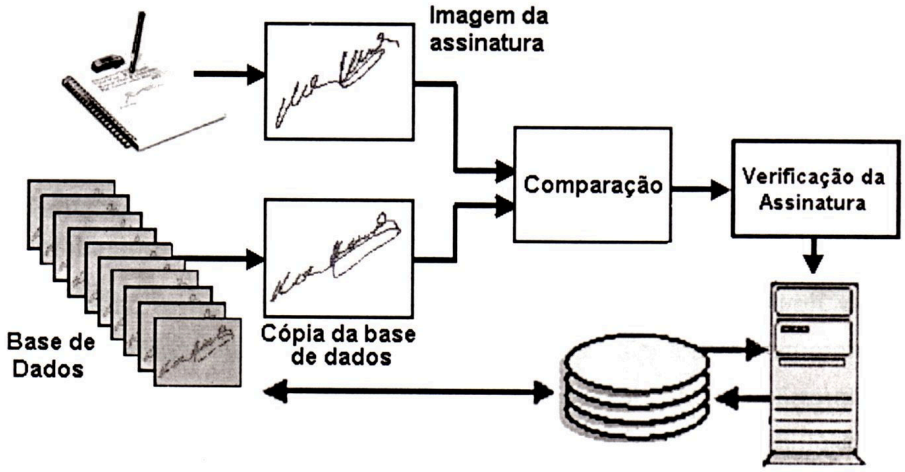


Figura 43 – RECONHECIMENTO ESTÁTICO DE ASSINATURA
Fonte: PINHEIRO (2008, pág. 81)

O sistema biométrico por reconhecimento da assinatura manuscrita tem um nível de segurança baixo, pois um impostor pode tentar falsificar a assinatura do usuário legítimo (CAMPOS, 2007). No entanto é uma técnica em constante aperfeiçoamento. Vale ressaltar que durante o ciclo de vida do usuário, à maneira do mesmo assinar é pouco provável de mudar. Porém existem alguns problemas ou situação para este tipo aplicação, tais como: se usuário legítimo estiver no momento nervoso ou sofrer de mal de Parkinson, não conseguirá ser identificado (PINHEIRO, 2008).

2.5 RESUMO E CONCLUSÕES SOBRE REVISÃO DA LITERATURA

O ENCAT cada vez mais tem se preocupado em melhorar de maneira eficaz o sistema de NF-e proporcionando unificação da informação entre as três esferas do governo, segurança, entre outros. Mas, diante dos fatos apresentados, ainda não é suficiente, pois o sistema de assinatura digital da NF-e não consegue em sua totalidade garantir o critério de autenticidade e não-repúdio.

Por outro lado, a ICP-Brasil tem feito sua parte, garantindo total segurança dos certificados digitais, fiscalizando suas AC's e acrescentando novas tecnologias em segurança da informação. Pode-se citar Silva (2008), ainda hoje, como uma das referências mencionadas em artigos científicos da atualidade, que demostram os procedimentos de segurança da hierarquia do ICP-Brasil. Porém, consta na revisão de literatura que as AC's exigem validação presencial do usuário, antes de emitir o certificado digital, e até exigem que o mesmo, assine

termo concordância, referente a ter cuidados e responsabilidade do detentor do certificado digital. Contudo isto ainda não é suficiente.

Ainda se tratando dos avanços tecnológicos, apenas ter um sistema computacional que utiliza criptografia assimétrica RSA não é suficiente, pois a mesma não garante que seja impossível de decifrar tal mensagem. Pesquisadores e autores como Boneh (2017) e Katz (2014) são referência para a criptografia moderna, e enfatizam a utilização de várias técnicas e combinações de algoritmos assimétricos em conjunto com algoritmos de resumo (*hash*), para dificultar a fatoração de números primos em tempo hábil.

Cada vez mais, tecnologia como *token* ou *smart card* estão presentes no nosso cotidiano, pois segundo Oliveira, (2015), estes dispositivos de segurança em *hardware* garantem a segurança de seus conteúdos. Contudo, não basta apenas utilizá-los, pois durante a pesquisa observou-se que a segurança do *token* ou *smart card* não garante por completo toda segurança de um sistema de autenticação, depende também da implementação da aplicação servidor (*applet*) e cliente (*host*).

Pesquisas como a de Nedjah, *et al.,* (2017), propõem a utilização da biometria como fator de autenticação do PIN. Já na visão de outros artigos, como o de Alejo (2016), não há a preocupação com os critérios de criptografia e a segurança do *template* durante a comunicação do *smart card* com a aplicação cliente (*host*).

Já no artigo acadêmico de Patil, et al., (2017), relata-se sobre a vulnerabilidade em sistemas de autenticação de vários fatores, no qual o usuário fornece vários meios de identificação, como *token* ou *smart card*, e o outro é tipicamente algo memorizado como PIN. Fato este que abrange novos desafios para o estado da arte e oportunidades de pesquisas para solucionar problemas em sistemas de autenticação de vários fatores e também sobre o uso dos certificados digitais, por pessoas que não sejam o proprietário real do mesmo.

No próximo capítulo são apresentados alguns trabalhos relacionados com a nossa proposta de solução, para eventuais comparações.

3 TRABALHOS RELACIONADOS

Neste capítulo são apresentados alguns trabalhos relacionados com a pesquisa desenvolvida nesta dissertação, com comparações e benefícios envolvidos:

- Manual de orientação do contribuinte v6.00 (ENCAT, 2015);
- *Efficient fingerprint matching on smart cards for high security and privacy in smart systems* (NEDJAH, et al., 2017);
- Criptografia no processo judicial eletrônico e na análise de provas digitais (SILVA, 2017);
- *Design and implementation of secure biometric based authentication system using RFID and secret sharing* (PATIL, et al., 2017);
- *Multiple application chip card having biometric validation* (PARTOUCHE, et al., 2012).

O manual de orientação do contribuinte v6.00 (ENCAT, 2015) é atualmente o padrão técnico para qualquer projeto de emissão de NF-e, onde se percebe que são necessários utilizar:

- Certificado digital tipo A3 emitido por uma AC;
- *Token* ou *smart card*;
- Criptografia;
- Internet.

Diante deste projeto, o fato de ser elegido pela SEFAZ e empresas, um órgão competente de uma AC, é de grande respaldo jurídico em relação a autenticidade de uma assinatura digital. Atualmente o ICP-Brasil, rege todos os padrões de segurança e fiscalizações em suas AC, referente a emissão dos certificados digitais, validades e utilização dos mesmos.

Quando a empresa solicita um certificado digital tipo A3, a própria AC escolhida disponibiliza o mesmo de forma pré-personalizado, com a senha padrão do PIN e PUK numérico “1234”, para posteriormente ser alterado. O dono do certificado digital, o cliente, assina um termo de compromisso da AC, e deveria guardar com segurança seu certificado digital, nem o compartilhá-lo com terceiros. Em geral, o cliente recebe uma cartilha informativa sobre demais procedimentos de segurança (SAFEWEB, 2015). Porém existe um grande problema:

> *The current authentication system uses manual methods like PIN and passwords which may be forgotten or be stolen and hence does not ensure that only the actual owner has access to it*. (PATIL, ET AL., 2017).

Já em relação ao projeto da NF-e (ENCAT, 2015), tanto a utilização do *token* ou *smart card*, garante a integridade dos dados contidos e a segurança do certificado digital, segundo normas da ISO 7816, o que é fundamental. Porém, o projeto não visa os procedimentos necessários de uma pré-autenticação, entre o programa de emissão da NF-e e do *token* ou *smart card*, evitando assim atender à solicitação de qualquer programa ilícito, através de comandos APU.

Na parte relativa à criptografia, sobre a utilização do algoritmo de resumo (SHA-1) e também com em conjunto com algoritmo RSA (1024 bits), são seguros dependendo do tempo de validade de um certificado digital que é de no máximo 3 anos, bem como, no projeto da NF-e é mencionado a transformação C14N que codifica para *base64*, dificultando assim para um invasor decrepitar em tempo hábil.

Mesmo utilizando o algoritmo RSA (1024 bits), existe um problema que no projeto da NF-e, não se preocupou sobre o critério de criptografia ser realizado dentro ou fora do *token* ou *smart card*. Fato este e real, que muitas aplicações de programas de emissão de NF-e, autorizadas pela SEFAZ, solicitam a chave privada e o certificado digital, para poder fazer todo processo de criptografia e demais procedimentos, fora do dispositivo de segurança (*token* ou *smart card*), falha esta que já acontece no certificado tipo A1.

Sendo assim, qualquer aplicação pode ter acesso ao conteúdo do mesmo, e até pior, alguns já armazenam o PIN numérico dentro do próprio emissor da NF-e, tornando possível que um invasor consiga capturar tanto a chave privada com seu PIN numérico e o seu certificado digital.

Já em relação ao meio de comunicação (internet) entre o emissor e destinatário, o modelo padrão SSL versão 3.0, é seguro e adotado também por outros projetos do governo federal.

No artigo *Efficient fingerprint matching on smart cards for high security and privacy in smart systems* (NEDJAH, et al., 2017), são mencionados os seguintes recursos:

- Biometria por reconhecimento de impressão digital;
- *Smart card*.

Neste aspecto a biometria por reconhecimento de impressão digital, demonstra-se cada dia mais seguro. Fato este que faz com que já sejam utilizados algoritmos avançados de reconhecimento das minúcias em conjunto com a tecnologia LFD, em vários leitores biométricos.

Em específico este artigo utiliza em sua proposta, um novo algoritmo avançado de captura e reconhecimento das minúcias, baseado no algoritmo SETA (*Skin Elasticity Tolerant Algorithm*), onde seus métodos de extração e comparação se demonstram ser mais eficazes do que outros algoritmos no estado da arte. Esta nova abordagem se torna muito útil para ser implementada nos sistemas de comparação de minúcias, dentro do *smart card*, chamado de MoC (*Match On Card*). A figura 44 apresenta seu modelo de comparação.

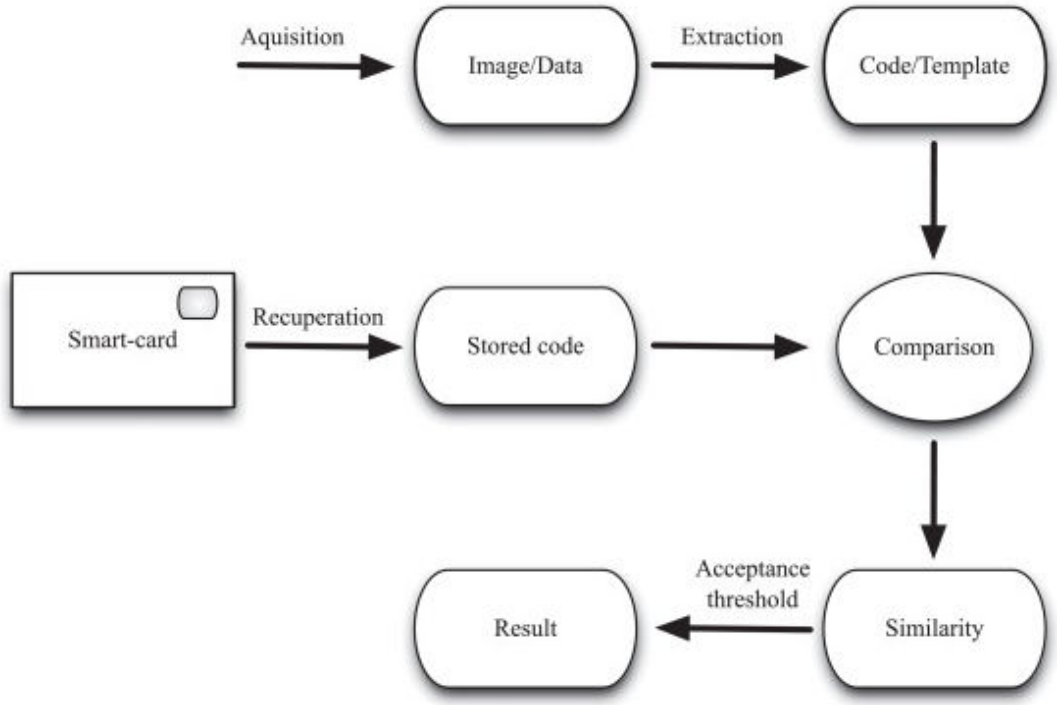


Figura 44 – BIOMETRIC VERIFICATION
Fonte: NEDJAH, ET AL., (2017)

Porém existe um problema na proposta, que toda a comunicação entre aplicação cliente (*host*) e aplicação servidor (*applet*) pode ser interceptada, pois não existe uma autenticação prévia e no *template* do usuário não existe nenhum tratamento de segurança, como por exemplo, o código de segurança do mesmo ou até criptografia, para evitar que algum invasor possa burlar o sistema de comparação.

Na monografia Criptografia no processo judicial eletrônico e na análise de provas digitais (SILVA, 2017), são utilizados os seguintes recursos:

- Certificado digital tipo A3 emitido por uma AC;
- *Token* ou *smart card*;
- Criptografia;
- Internet.

Esta abordagem possui caraterísticas similares àquelas do projeto de emissão de NF-e (ENCAT), porém com algumas diferenças. Sua proposta procurou utilizar bastante respaldo jurídico em relação a confidencialidade, integridade, autenticidade e não-repúdio, o qual é fundamental em qualquer sistema computacional que utiliza processo de assinatura eletrônica. No entanto todo este respaldo jurídico em seu modelo proposto de assinatura digital não garante que o documento assinado de fato foi realizado pelo usuário legítimo do *token* ou *smart card*, que contém sua chave privada e seu certificado digital. Com isso percebe-se que tal proposta, apresenta os mesmos problemas mencionados anteriormente, sobre o processo de assinatura digital da NF-e, como também referente aos procedimentos de emissão do certificado tipo A3.

Vale ressaltar que no sistema web do TJPE, referente a autenticação e assinatura digital, sempre é solicitado que o usuário digite manualmente seu respectivo PIN numérico, porém mesmo assim, já que é acionado pela aplicação a DLL do *token* ou *smart card*, acaba sendo enviado para a classe *KeyStore*, a chave privada e seus respectivo PIN para o processo de criptografia, onde é passível de uma tentativa de captura do mesmo.

No artigo *Design and implementation of secure biometric based authentication system using RFID and secret sharing* (PATIL, et al., 2017), são mencionados os seguintes recursos:

- Reconhecimento de imagem biométrica por impressão digital ou íris;
- *Smart card* RFID.

Neste artigo o autor propõe, dividir o *template* biométrico em duas partes, ou seja, uma no *smart card* RFID e a outra no banco de dados do servidor da aplicação.

Quando o usuário deseja se autenticar, o algoritmo da aplicação extrai do *smart card* RFID e do servidor de banco de dados, as partes das imagens para reconstruir o *template* biométrico por completo. Posteriormente utiliza-se um scanner biométrico para captura das características da impressão digital ou íris, para compará-las com o *template* biométrico fornecido pela aplicação. Se os *templates* biométricos forem iguais, o usuário será autenticado.

A figura 45 apresenta o modelo de sistema de autenticação.

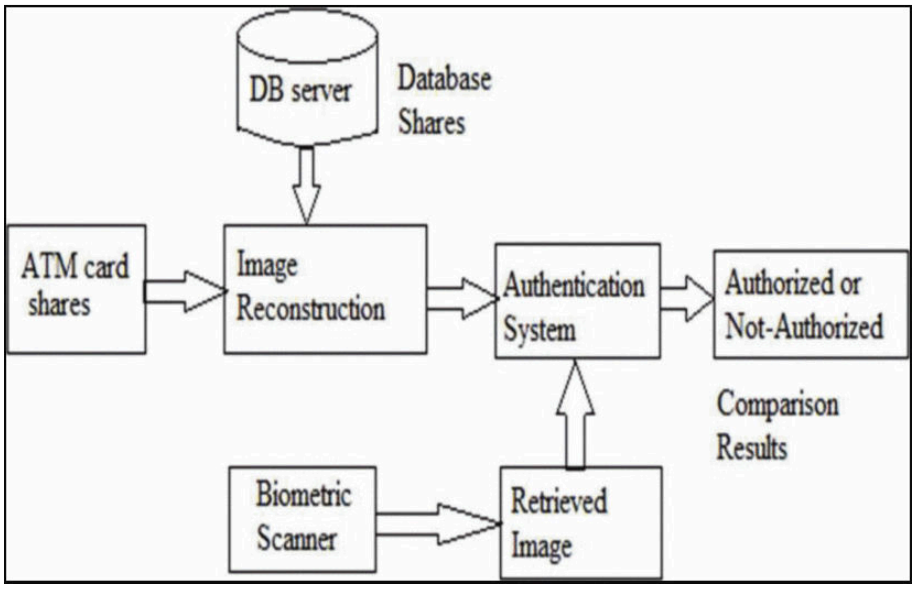


Figura 45 – BIOMETRIC BASED AUTHENTICATION SYSTEM
Fonte: PATIL, ET AL., (2017)

Porém existe um problema na proposta, pois o sistema da aplicação não utiliza uma autenticação prévia entre as partes, *smart card* RFID e o servidor do banco de dados. Outro fator a mencionar é que a comunicação da captura do *template* do usuário até o sistema de autenticação, não possui tratamento de segurança, como por exemplo código de segurança do mesmo ou até criptografia, para evitar que algum invasor possa burlar o sistema de comparação.

Por último, na patente de *Multiple application chip card having biometric validation* (PARTOUCHE, et al., 2012), utiliza-se os seguintes recursos:

- *Smart card* com chip multiplicativo por contato ou sem contato RFID para verificação biométrica.

O objetivo da invenção do novo modelo de *smart card* por contato ou sem contato RFID foi de fornecer uma solução alternativa às soluções existentes, para proteger a informação contida do mesmo, como por exemplo *templates* biométricos, e entre outros. Sendo assim, tal modelo proposto do chip multiplicativo, poderia atender a múltiplas funções e ser acionado tal aplicativo dependendo da localização do ambiente em que se encontra o mesmo.

Pode-se observar, na figura 46, seu modelo de sistema de autenticação.

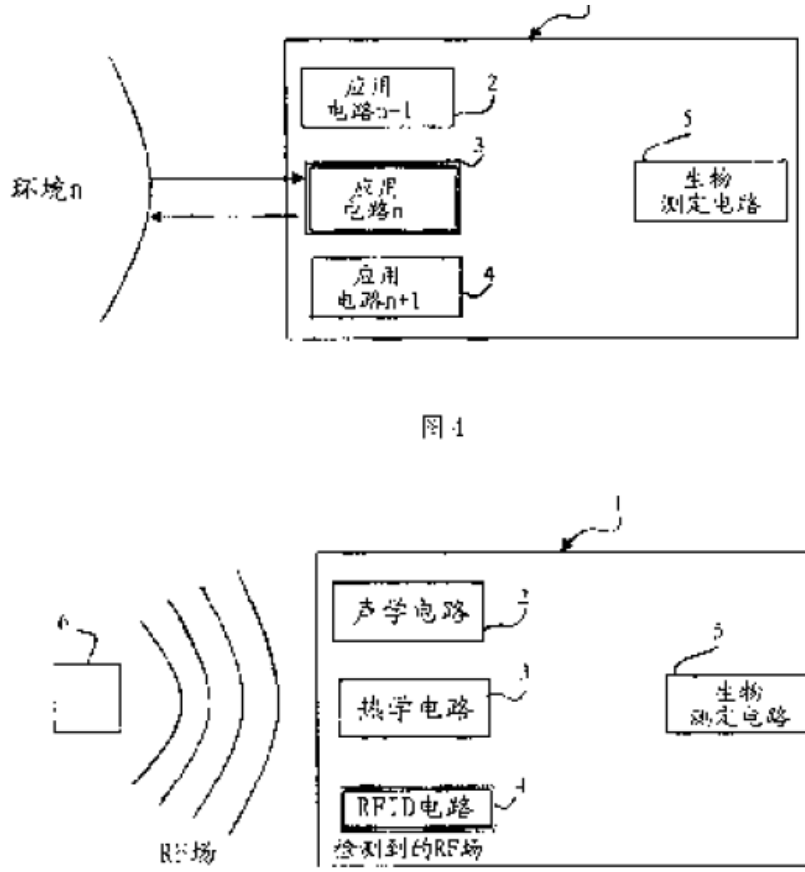


Figura 46 – MULTI-APPLICATION CHIP CARD WITH BIOMETRIC VERIFICATION
Fonte: PARTOUCHE, et al., (2012)

Porém existe um problema na proposta da invenção, que toda a comunicação entre aplicação cliente (*host*) e aplicação servidor (*applet*) pode ser interceptada, pois não existe uma autenticação prévia entre as partes e nem utiliza criptografia. Percebe-se outro problema que poderia ocorrer durante a comunicação da captura do *template* do usuário até o sistema de autenticação interno ou externo do *smart card* RFID; não foi mencionado nenhum tratamento de segurança, como por exemplo, código de segurança do mesmo ou até criptografia, para evitar que algum invasor possa capturar o *template* biométrico e com isso burlar o sistema de comparação.

Por fim, na tabela 15 da seção 5.4 descreve-se o quadro comparativo dos trabalhos relacionados com a proposta de solução desta pesquisa.

4 METODOLOGIA DE DESENVOLVIMENTO DO PROJETO

Neste capítulo é descrita em detalhes a metodologia proposta nesta pesquisa científica.

Para atingir os objetivos propostos, esta pesquisa científica é de caráter exploratória e descritiva.

O objetivo da pesquisa exploratória é:

> Proporcionar maior familiaridade com o problema (explicitá-lo). Pode envolver levantamento bibliográfico, entrevistas com pessoas experientes no problema pesquisado. (GIL, 2008).

No que se refere a descritiva:

> A pesquisa descritiva é caracterizada pelo levantamento de dados e pela aplicação de entrevistas e questionários. (WAZLAWICK, 2014).

Quanto aos meios de procedimentos técnicos, a pesquisa foi experimental, pois segundo Wazlawick (2014), uma pesquisa experimental "implica ter uma ou mais variáveis experimentais que podem ser controladas pelo pesquisador (o fato de usar ou não determinada técnica, por exemplo), e uma ou mais variáveis observadas, cuja medição poderá levar, possivelmente, à conclusão de que existe algum tipo de dependência com a variável experimental...".

Quanto à forma de abordagem, esta foi quantitativa, pois segundo Boenti (2004), "pesquisa quantitativa é quando há levantamento, quantificação e mensuração de resultados, visando avaliar quantidades".

4.1 ESTRUTURA METODOLÓGICA

Foi adotada uma abordagem filosófica positivista, onde dentro de uma população de 40 empresas de pequeno e médio portes, que atuam nas proximidades do centro comercial da cidade de Caruaru-PE, foi selecionada uma amostra do problema real de 20 empresas, na qual foi constado o mesmo tipo de problema de segurança da informação, quanto ao compartilhamento e a legitimidade do uso do certificado digital tipo A3, pelo proprietário.

No que se refere à pesquisa exploratória, realizamos no capítulo 2, um levantamento bibliográfico da NF-e, procurando obter informações e conceitos sobre o sistema atual da assinatura digital da NF-e, certificação digital (ICP-Brasil), *smart card*, bem como, as novas tendências de sistemas tecnológicos baseados em biometria (LFD).

Para efeito de comparação no capítulo 4, aborda-se alguns dos principais trabalhos relacionados com nosso projeto.

No capítulo 5, demonstra-se a identificação do problema, no cenário atual do processo de assinatura eletrônica da NF-e, bem como, o projeto de Autenticação Multifatorial em *Hardware* e seu fluxograma de inclusão, no cenário do processo da assinatura digital da NF-e. Posteriormente, será descrito como é o modelo do cenário de simulação, para a realização do quase experimento, utilizando como variável de controle, com ou sem a utilização do *hardware* biométrico, em conjunto com o *smart card*. Já no capítulo 6, demonstra-se as limitações desta pesquisa.

Segundo o IBGE (2016), no Brasil cerca de 96,3% das empresas de comércio são de pequeno ou médio porte, onde uma das características de classificação das empresas de pequeno porte é ter em seu quadro funcional de 1 até 49 funcionários, e de médio porte é ter de 50 até 99 funcionários (SEBRAE, 2016).

Assim, justificando-se a parte descritiva e quantitativa da pesquisa, procurou-se escolher de forma aleatória, entre 40 empresas de pequeno e médio portes, as que atuam nas proximidades do centro comercial da cidade de Caruaru-PE, e que emitem NF-e, 20 empresas, dentre elas:

- 10 Empresas de pequeno porte, na área de comércio (vestuário, eletrodoméstico, informática, supermercado, material de construção e revendedor de peças automotivas);
- 8 Empresas de pequeno porte, na área de prestação de serviços (escritório de advocacia, clínica médica, escritório de contabilidade, assistência técnica de informática e eletrônica);
- 1 Empresa de médio porte, na área de comércio (vestuário);
- 1 Empresa de médio porte, na área de prestação de serviços (segurança patrimonial).

Estas empresas voluntárias permitiram a realização desta pesquisa através de consentimento dos seus proprietários e funcionários, para participaram anonimamente e de forma voluntária. Os proprietários das empresas e seus respectivos funcionários, responsáveis por emitirem NF-e, totalizaram em 30 pessoas, as quais permitiram ser observadas durante seu

expediente de trabalho, a fim de que fosse possível a coleta adequada dos dados e posterior análise.

Para enfatizar mais a pesquisa, foi apresentada uma carta de apresentação (Apêndice A), para os 30 participantes, bem como, um questionário (Apêndice B) de múltipla escolha, sobre questões referentes ao impacto da NF-e da vida da empresa, em questões como: segurança, autenticidade e não-repúdio do modelo atual da assinatura digital da NF-e.

Sendo assim, foram coletados dados, sem interferir no cotidiano de cada empresa durante o período de 22 meses, para se estabelecer uma métrica de segurança da informação, em relação ao novo modelo proposto de autenticação. Após isso, foi realizado, um quase experimento, utilizando Autenticação Multifatorial em *Hardware*, em conjunto com um leitor biométrico e o *smart card*, em um ambiente simulado. Nesta fase foram convidadas as mesmas pessoas, das 20 empresas escolhidas, para participaram anonimamente ou não, e de forma voluntária do experimento, e verificar se os mesmos conseguiriam burlar a autenticação de impressão digital (LFD), passando-se por outra pessoa, para efetuar a assinatura digital da NF-e.

Com isso, foi possível estabelecer um comparativo, demonstrado no capítulo 5, entre o modelo atual de assinatura digital da NF-e, que utiliza seu *hardware token* ou *smart card* em conjunto com seu respectivo PIN, e o modelo proposto neste projeto, qual seja, a Autenticação Multifatorial em *Hardware*, em conjunto com o leitor biométrico e o *smart card*.

4.2 CRONOGRAMA DA PESQUISA

A figura 47 apresenta o cronograma de desenvolvimento do projeto de pesquisa até sua conclusão, em relação aos meses de cada etapa. Na tabela 7 descreve-se o significado das siglas utilizadas.

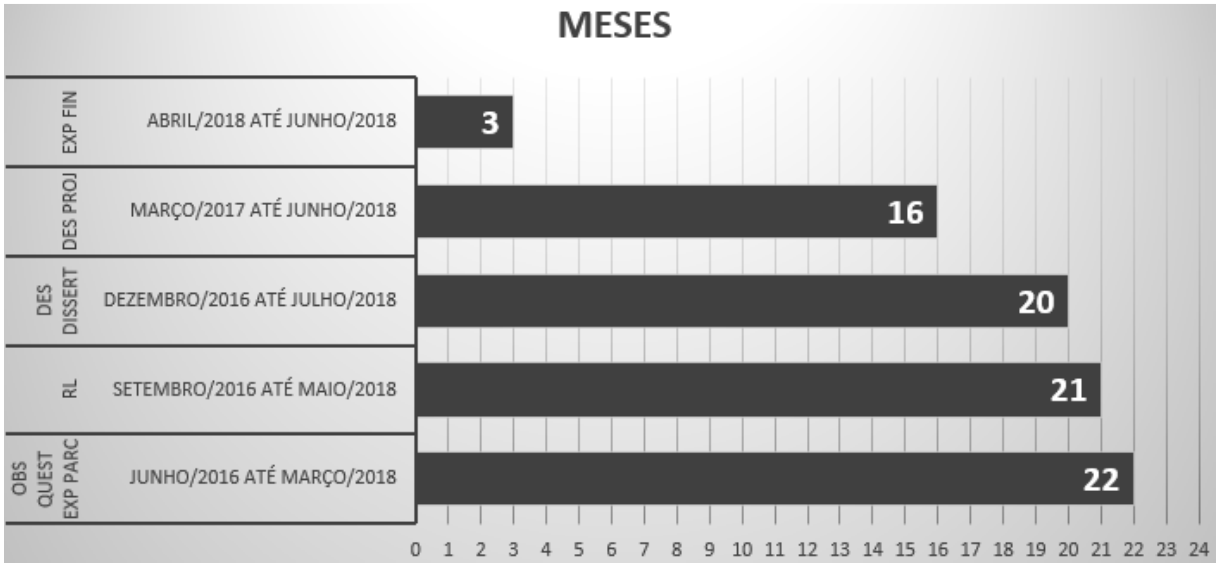


Figura 47 – CRONOGRAMA DO PROJETO DE PESQUISA

Fonte: FIGURA REALIZADA PELO AUTOR

Tabela 7 – SIGNIFICADO DAS SIGLAS

Sigla	Significado
EXP FIN	Experimento Final
DES PROJ	Desenvolvimento do Projeto
DES DISSERT	Desenvolvimento da Dissertação
RL	Revisão da Literatura
OBS / QUEST / EXP PARC	Observação / Questionário / Experimento Parcial

Fonte: TABELA REALIZADA PELO AUTOR

5 AUTENTICAÇÃO MULTIFATORIAL EM *HARDWARE* PARA O PROCESSO DE ASSINATURA DIGITAL DA NF-e

Este capítulo descreve a proposta de solução para as hipóteses citadas no tópico 5.1. Em seguida, no tópico 5.2 é apresentado um comparativo entre as tecnologias existentes, a fim de justificar qual delas se enquadra melhor, visando um aumento do nível de segurança do processo de emissão da NF-e.

A figura 48 apresenta o fluxo de tarefas realizadas dentro de um caso de uso na perspectiva do usuário da AC:

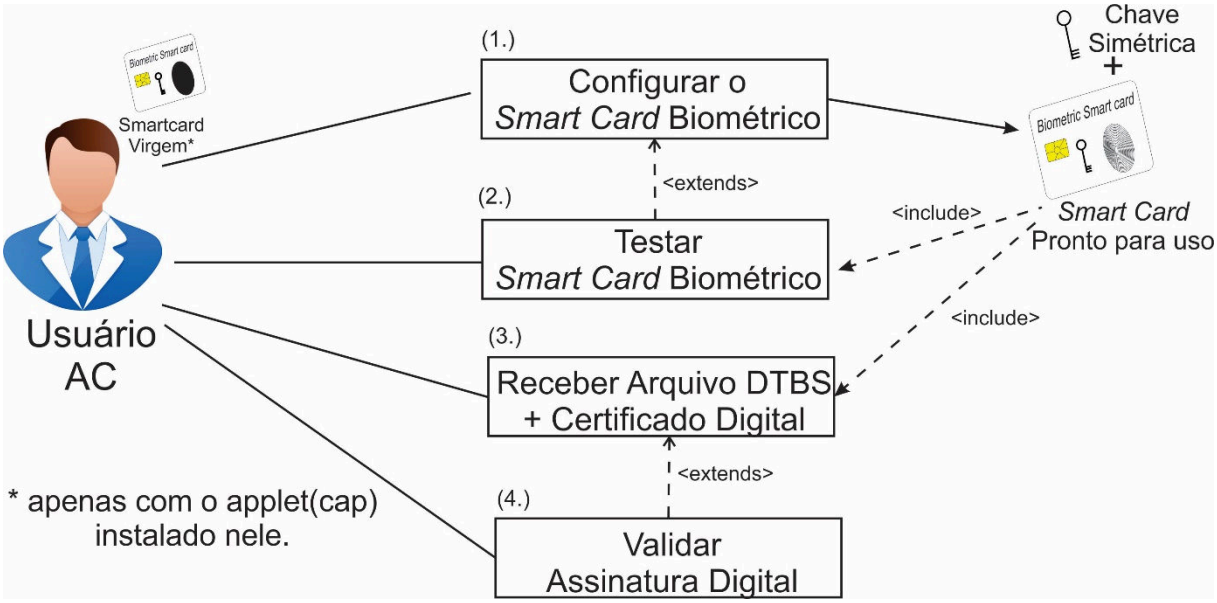


Figura 48 – VISÃO MACRO (PERSPECTIVA DO USUÁRIO DA AC)
Fonte: FIGURA REALIZADA PELO AUTOR

Descrição das tarefas:

1. Configurar o *smart card* biométrico, de forma personalizado, colocando-o dentro a aplicação servidor (*applet*): inserir o PIN biométrico, chave simétrica, chaves privadas e públicas. Por fim, entregar o *smart card* biométrico e a chave simétrica da aplicação cliente (*host*), para o usuário final;
2. Testar *smart card* biométrico – Verificar o *smart card* biométrico, antes de entregá-lo ao usuário final;
3. Receber arquivo DTBS + certificado digital – Receber do usuário final o arquivo assinado e seu certificado digital;

4. Validar assinatura digital – Validar assinatura digital do documento assinado, bem como verificar a validade do certificado digital utilizado.

No item 5.3, suas funções: configuração do *java card* biométrico pela AC e validação da assinatura pela AC, são descritas em detalhes.

A figura 49 apresenta o fluxo de passos existentes em um caso de uso típico, na perspectiva do usuário final:

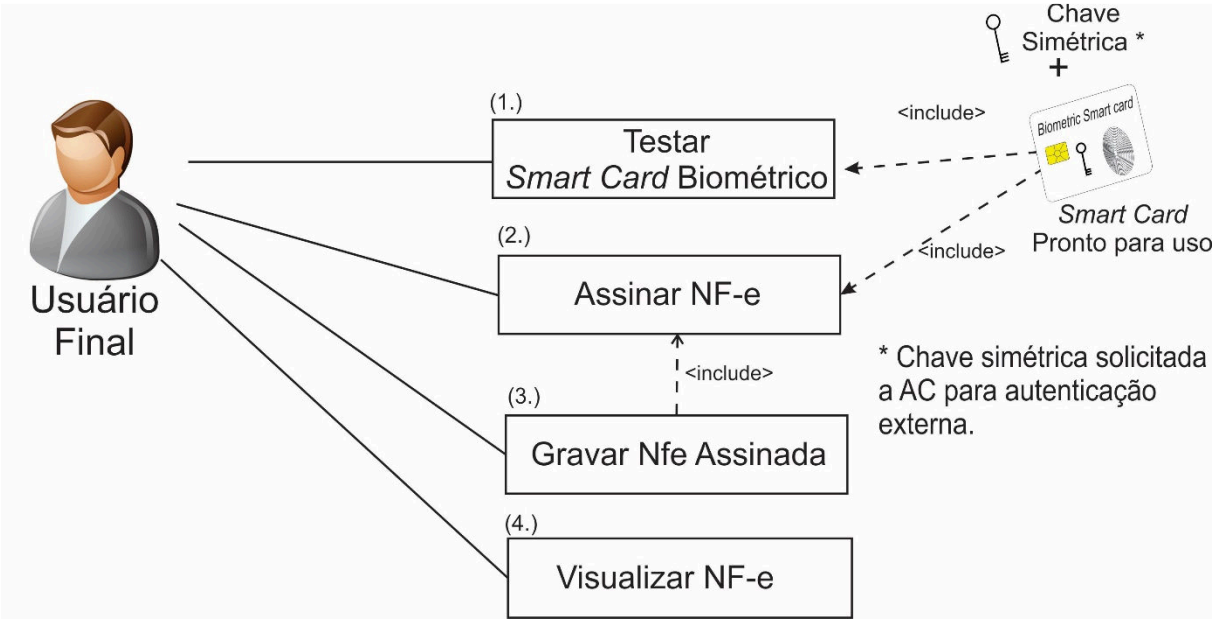


Figura 49 – VISÃO MACRO (PERSPECTIVA DO USUÁRIO FINAL)

Fonte: FIGURA REALIZADA PELO AUTOR

1. Testar *smart card* biométrico – Testar *smart card* biométrico em conjunto com AC;
2. Assinar NF-e – Assinar arquivo XML;
3. Gravar NF-e assinada – Gerar NF-e do arquivo XML assinado;
4. Visualizar NF-e – Visualizar a NF-e, verifica-la se está assinada e imprimir.

No tópico 5.3 cada função: configuração do *java card* biométrico pela AC e emissão da NF-e, será descrita em detalhes.

Na figura 50 pode ser visualizado o fluxo típico de um caso de uso na perspectiva do usuário final:

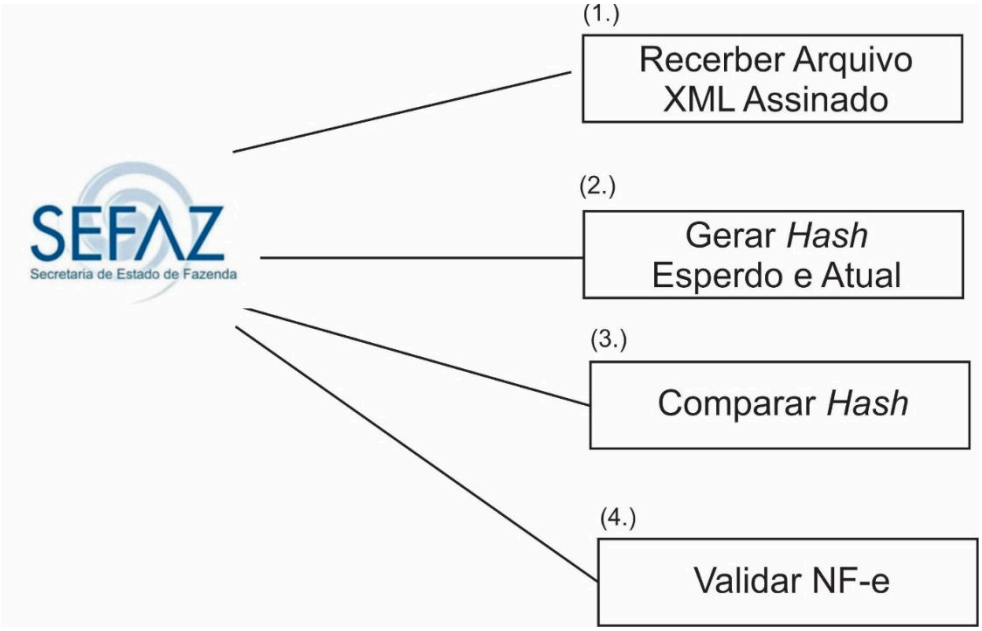


Figura 50 – VISÃO MACRO (PERSPECTIVA DA SEFAZ)

Fonte: FIGURA REALIZADA PELO AUTOR

1. Receber arquivo XML assinado – Receber arquivo XML assinado pelo emitente;
2. Gerar *hash* esperado e atual – Gerar *hash* esperado e atual;
3. Comparar *hash* – Comparar *hash*;
4. Validar NF-e – Validar NF-e e armazena-la em repositório.

O item 5.3 trata em detalhes esta função: validação da NF-e pela SEFAZ.

No item 5.4 verifica-se análise dos resultados e comprovação da eficácia do nosso modelo proposto. No item 5.5 são analisados seus benefícios.

5.1 SEGURANÇA, AUTENTICIDADE E NÃO-REPÚDIO DA EMISSÃO DA NF-e

Conforme já abordado no referencial teórico, o ambiente computacional da NF-e demonstra ser seguro. Porém para a realização da análise deste ambiente, há a necessidade de se retomar as etapas do processo de emissão de NF-e, as quais estão de acordo com o Manual de Integração – Contribuinte versão 6.00 desenvolvido pelo ENCAT em setembro de 2015:

1. Quando o emitente (empresa) faz uma NF-e é gerado um arquivo eletrônico (XML), contendo as informações fiscais da operação comercial.

1.1 Este arquivo eletrônico (XML) ao tentar ser transmitido pela internet, por HTTPS e SSL versão 3.0 com autenticação mútua, para o servidor da SEFAZ (jurisdição do contribuinte emitente), o próprio aplicativo do emitente solicita a sua assinatura digital.

1.2 Então, para assinar digitalmente com a chave privada do emitente, é necessário utilizar o dispositivo de segurança (*token* em PC, *token* em *hardware* ou *smart card*) e colocar a sua respectiva senha (PIN), os quais servem para garantir a autoria e a integridade dos dados.

1.3 Após o emitente assinar digitalmente, esta é anexado ao arquivo eletrônico (XML), junto com a chave pública do certificado do usuário final. Em seguida o aplicativo do emitente transmite o arquivo eletrônico (XML) pela internet, por HTTPS e SSL versão 3.0 com autenticação mútua, para o servidor da SEFAZ (jurisdição do contribuinte emitente), utilizando-se assim a tecnologia de criptografia de dados por chave assimétrica.

2. Ao receber o arquivo eletrônico (XML), o servidor da SEFAZ (jurisdição do contribuinte emitente), faz a validação do mesmo. Vale informar que nesta etapa de validação, o servidor utiliza a chave pública do emitente para descriptografar os dados.

3. Após isto, é enviado o resultado desta validação para o emitente, ou seja, se a recepção do mesmo estiver tudo OK segue-se para a próxima etapa, se não, uma mensagem de erro é enviada para o aplicativo do emitente.

4. Se tudo ocorreu sem erro, a autorização de uso da NF-e é devolvida ao aplicativo do emitente.

5. Finalmente, é possível imprimir o DANFE (Documento Auxiliar da Nota Fiscal Eletrônica).

Serão analisadas apenas as seguintes etapas 1.1, 1.2 e 1.3 do processo de emissão de NF-e, onde serão abordados seus pontos positivos ou negativos, em relação à segurança, autenticidade, não-repúdio e integridade. No quesito de segurança, insere-se os serviços de confidencialidade, integridade e disponibilidade: com relação ao quesito de autenticidade, deve-se garantir que o solicitante seja realmente quem diz ser, baseando-se pelas suas credenciais, e no quesito de não-repúdio, tem que garantir que nenhuma das partes envolvida

na comunicação possa negar falsamente a sua participação em qualquer momento da comunicação (PEREIRA, 2016).

Na etapa 1.1 do processo de emissão da NF-e, percebe-se um ponto positivo em relação à segurança: a comunicação entre a empresa e a SEFAZ, utiliza os protocolos HTTPS e o SSL versão 3.0 para garantir um túnel de comunicação seguro dentro da internet (ENCAT, 2016). Isto garante a impossibilidade de invasão e interceptação da comunicação.

Na etapa 1.2 do processo de emissão da NF-e, percebe-se um grande ponto negativo em relação à autenticidade. A fim de identificá-lo, há a necessidade de se observar como esta etapa ocorre. Segue sua descrição: quando é efetuada a assinatura digital pelo emissor (empresa) através de seu certificado digital tipo A1 (*token* em PC) ou A3, com seu dispositivo de segurança (*token* em *hardware* ou *smart card*) em conjunto com sua senha PIN, tal tecnologia não garante que o proprietário do certificado digital, seja realmente o legítimo dono do mesmo (BORTOLINI, 2017).

Este fato em particular foi observado de forma presencial e também através de questionário, durante o expediente de trabalho dos nossos participantes da pesquisa, sem interferir em suas atividades profissionais. Como resultado da pesquisa foram coletados os seguintes dados:

- 73% das empresas não têm nenhuma política de segurança da informação (PSI) e 27% delas têm PSI, porém não aplica as normas da ISO 27002:2013 (ABNT, 2013) de forma correta;
- 83% destas empresas não conseguem garantir autenticidade e não-repúdio de uma NF-e, ou seja, se de fato foi emitida pelo usuário legítimo do certificado digital. Já o restante dos 17% consegue garantir a legitimidade da NF-e, devido o próprio usuário do certificado digital ser responsável por toda emissão da NF-e;
- 68% das empresas já tiveram problemas de não saber como responsabilizar, o usuário que emitiu uma NF-e indevidamente. Tal problema não ocorreu com os outros 32%;
- 85% dos funcionários utilizam a senha padrão do PIN numérico “1234” para o *smart card* ou *token* e os outros 15% utilizam a senha de algum sistema de autenticação igual ao PIN numérico;
- 77% dos funcionários deixam o seu *smart card* ou *token* conectado na leitora, mesmo que saiam para almoçar ou até mesmo de um dia para outro. Os outros 23% deixam o *smart card* dentro de uma gaveta sem fechadura;

- 81% dos funcionários sempre compartilham a senha PIN, do *smart card* ou *token* com os demais, para que possam também emitir NF-e. O restante dos 19% não compartilham com outros funcionários devido a não necessidade;
- 92% dos funcionários sempre compartilham o *smart card* ou *token* e seu PIN com o proprietário da empresa, contador e também com o suporte do programa de emissão da NF-e;
- 79% das empresas, em seus programas de emissão da NF-e, já armazenam o parâmetro do PIN (*token* ou *smart card*), para que o funcionário não precise digitá-lo. Já os 21% restante das empresas utilizam o próprio emissor gratuito da SEFAZ, o qual solicita a digitação do PIN ou o seu próprio programa de emissão de NF-e não tem este recurso de armazenar o PIN.

Sendo assim, neste sistema computacional, observa-se que o elo mais fraco é o usuário. Neste contexto pode-se observar a ocorrência de uma das seis hipóteses abaixo, em relação ao problema apresentado:

- Primeira hipótese – Quando um usuário solicita um certificado digital tipo A1 por alguma autoridade certificadora (AC) credenciada pela ICP-Brasil é comum no momento da geração do par de chaves (privada e pública), as quais serão instaladas no PC do usuário, serem colocadas pelo próprio titular do *token* em PC, sua respectiva senha confidencial. Porém se o *PC* do usuário estiver infectado com algum tipo de programa espião como é o caso do *spyware*, sua identidade digital pode ser comprometida e violada. Ou seja, o invasor com certo conhecimento de programação e segurança em redes poderá copiar o arquivo criptográfico que contém o par de chaves (privada e pública) e até mesmo capturar a senha do usuário para se passar pelo usuário legítimo (VIEIRA, 2007);
- Segunda hipótese – Quando um usuário solicita um certificado digital tipo A1 por alguma autoridade certificadora (AC) credenciada pela ICP-Brasil é comum no momento da geração do par de chaves (privada e pública), o qual será instalada no computador do usuário, ser colocado pelo próprio titular do *token* em PC sua respectiva senha confidencial, como por exemplo, “1234”, ano de nascimento e entre outros, tendo em vista de ser uma senha fácil de lembrar. Sendo assim, o invasor não precisa ser um perito em informática para se passar pelo usuário legítimo, pois se o mesmo conseguir em algum momento acessar localmente o PC do usuário e utilizar

o seu certificado digital que se encontra no PC, a primeira coisa que vai fazer quando o sistema solicitar a senha do *token* em PC é tentar colocar tipos de senhas padrões (exemplo “1234”), procurar na agenda do usuário por anotações de senhas, e até mesmo antes de invadir o PC poderá tentar visualizar a digitação da senha pelo usuário ou ouvir a senha do mesmo em alguma determinada ocasião (PINHEIRO, 2008);

- Terceira hipótese – O usuário ao solicitar um certificado digital tipo A3 por alguma autoridade certificadora (AC) credenciada pela ICP-Brasil é comum no momento da geração do par de chaves (privada e pública) serem colocados pelo próprio titular do *token* em *hardware* ou *smart card* o seu PIN e PUK, como por exemplo, “1234”, ano de nascimento e entre outros, tendo em vista de serem senhas fáceis de lembrar ou até mesmo para facilitar possíveis manutenções pelos administradores de TI. Sendo assim, o dispositivo de segurança (*token* em *hardware* ou *smart card*) por ser portátil, tem a fragilidade de poder ser roubado, furtado ou até mesmo perdido pelo usuário, com isso, o invasor não precisa ser um perito em informática para se passar pelo usuário legítimo, pois se o mesmo estiver de pose do *token* em *hardware* ou *smart card,* a primeira coisa que vai fazer quando o sistema solicitar o PIN é tentar colocar tipos de senhas padrões (exemplo “1234”), procurar na agenda do usuário por anotações de senhas, e até mesmo antes de invadir poderá tentar visualizar em alguma ocasião a digitação do PIN pelo usuário ou ouvir alguma conversar em relação a este assunto (PINHEIRO, 2008);
- Quarta hipótese – Quando um certificado digital tipo A1 (*token* em PC) ou A3 (*token* em *hardware* ou *smart card*) em conjunto com sua respectiva senha (PIN) for compartilhado com várias pessoas, isto poderá acarretar problemas futuros. Sendo assim, uma vez que o certificado digital é compartilhado, o dono da empresa não conseguirá identificar qual funcionário se utilizou de forma ilícita para gerar NF-e;
- Quinta hipótese – É muito comum que uma boa parte das empresas de software comercializam programas de emissão de NF-e, no qual o código fonte do mesmo, aciona o método *KeyStore* e acaba armazenando o PIN do A3 (*token* ou *smart card*) dentro do próprio computador do cliente. Isto facilita o dia a dia do funcionário, pois o mesmo não tem a necessidade neste caso de digitar o PIN ao assinar qualquer NF-e. Isto é um problema muito sério, pois como o PIN fica gravado no computador e armazenado por alguma variável do programa de emissão da NF-e, qualquer pessoa

pode se passar pelo usuário legítimo do *token* ou *smart card*. Fato este que a maioria das empresas deixam o *token* ou *smart card*, sempre conectado no computador.

- Sexta hipótese – Uma boa parte de livros e códigos fontes distribuídos pela internet, para desenvolvimento do modelo de programas de emissão de NF-e, demonstra que no código fonte do mesmo, a aplicação cliente solicita a chave privada do certificado tipo A3, para ser armazenada no método *KeyStore*, junto com seu respectivo PIN, para posteriormente assinar a NF-e. Diante deste fato, acaba o certificado tipo A3 virando um certificado tipo A1, pois facilita um invasor copiar o mesmo com seu respectivo PIN, ao mesmo tempo.

Qualquer uma das seis hipóteses mencionadas acima poderá causar um prejuízo enorme para qualquer empresa de pequeno ou médio porte, e até a falência da mesma. Pois, se o invasor, ou até mesmo um funcionário da empresa tendo a possibilidade de se passar pelo usuário legítimo do certificado digital, detiver alguma mercadoria com documentação irregular ou até furtada, pode-se gerar notas fiscais sem o consentimento do dono da empresa. Desta forma, pode-se vender e transitar tal mercadoria em vários estados brasileiros e até fora do Brasil de "forma legal", tendo em vista que as respectivas mercadorias possuem suas respectivas NF-e.

Sendo assim, analisando este cenário, percebe-se claramente a empresa só terá conhecimento do desfalque quando da realização de alguma auditoria contábil detalhada. Neste caso, poder-se-á verificar pagamentos de impostos de NF-e indevidos de mercadorias que não fazem parte do seu estoque real da empresa.

Com resultado deste processo ilícito, a empresa pode ser penalizada por efetuar pagamento de impostos sem sua anuência, bem como, ser multada pela SEFAZ por sonegação de impostos (ICMS). Esta multa pode variar de 10% a 100% sobre valor da NF-e (MARCHIORO, 2011).

Na etapa 1.3 do processo de emissão da NF-e, percebe-se um ponto positivo em relação a não-repúdio, pois este é eleito entre as partes: empresa x SEFAZ, denominado de ICP-Brasil. O não-repúdio rege os padrões de segurança das unidades certificados (AC), capaz de garantir total segurança da geração do par de chaves criptográfico únicos, confiabilidade e privacidade do mesmo (VIEIRA, 2007).

Sendo assim, ao ser assinado digitalmente a NF-e, não tem como a empresa dizer que não reconhece tal assinatura digital, pois somente ela é detentora desta assinatura digital única e é de sua responsabilidade guardá-la em segurança contra os possíveis invasores. Desta forma a NF-e tem validade jurídica e irrevogável. Quando o empresário emite uma NF-e, seus dados

são enviados para o servidor da SEFAZ, onde constará uma chave de registro, pelo qual o remetente, que enviou e assinou a NF-e digitalmente através do seu certificado digital, garante sua autoria e integridade.

Para a solução do problema existente na etapa 1.2, do processo de emissão da NF-e, mencionada anteriormente, é apresentada uma proposta de solução para o problema do uso não autorizado do certificado tipo A3; apenas do dispositivo de segurança s*mart card* em conjunto com seu respectivo PIN biométrico.

5.2 COMPARAÇÃO ENTRE TECNOLOGIAS

Sabe-se que para que um sistema computacional seja válido pelos padrões de segurança internacional, conforme já abordado anteriormente, são necessários no mínimo dois tipos de fatores de autenticação (KERBY, 2012).

Segundo Matos (2003), em um dos estudos realizados pelo grupo de teleinformática e automação da UFRJ, publicou que:

> A tecnologia do *smart card* reforça a integridade das aplicações de correio segura já que a chave privada é armazenada diretamente sobre o cartão, o qual é protegido por um código confidencial. Para se apropriar da chave privada de um usuário e enviar mensagens em seu nome, é necessário não somente possuir *smart card* desse usuário, mas também reconhecer seu código confidencial. Pode-se mesmo imaginar que esse código confidencial seja substituído pelo modelo biométrico de uma impressão digital de um usuário, reforçando ainda as garantias de não-repúdio da mensagem protegida por uma assinatura eletrônica. (MATOS, 2003)

Nesta proposta, para solucionar o problema de segurança, autenticidade e não-repúdio do processo de assinatura da NF-e, são utilizados dois fatores de autenticação (algo que se tem + algo que você é) durante a assinatura digital da NF-e.

Na escolha do primeiro fator de autenticação (algo que se tem), se faz necessário realizar um comparativo entre os diversos dispositivos de segurança, aos quais são demonstrados e comparados entre si na tabela 8.

Tabela 8 – COMPARAÇÃO ENTRE OS DISPOSITIVOS DE SEGURANÇA

Dispositivo de Segurança	Tipo de Certificado Digital	Necessita de Leitora	Identificação Impressa	Desempenho Computacional	Nível de Segurança
Token em PC	A1	Não	Não	Rápido	Baixo
Token em *hardware*	A3	Não	Não	Lento	Médio
Etoken	A3	Não	Não	Lento	Alto
Smart Card	**A3**	**Sim**	**Sim**	**Lento**	**Alto**

Fonte: TABELA REALIZADA PELO AUTOR (BASEADO NOS TÓPICOS 2.3.1 E 2.3.2)

O *etoken* como o *smart card*, tem capacidade de armazenar o certificado tipo A3 (chave privada e chave pública) e o *template* biométrico de impressão digital, com tamanho de 256 a 669 bytes. Ambas as tecnologias podem garantir aos certificados tipo A3 um armazenamento inviolável das chaves (pública e privada) entre outras informações pessoais, desde que o mesmo isole o cálculo crítico de segurança relativo à troca de chaves, autenticação e a assinatura eletrônica (SILVA, et al., 2008).

Partindo do comparativo apresentado na tabela 8, para o fator de autenticação “algo que se têm” foi escolhido à tecnologia do *smart card*, mais especificamente o *java card* com capacidade de 80 Kb, mesmo tendo-se a necessidade de se adquirir uma leitora, com custo estimado em R$50,00. Esta opção tem uma vantagem em relação ao *etoken*, que seria a possibilidade da colocação impressa no próprio *smart card*, da identificação dos dados do usuário ou empresa, bem como, prover a possibilidade de se utilizar a tecnologia *smart card hybrid ou combi* para diferentes aplicações.

A fim de escolher o segundo fator de autenticação (algo que você é), faz-se necessário observar nas tabelas 9, 10 e 11, critérios, tais como: invasivo, nível de segurança, custo e entre outros.

A tabela 9, apresenta a comparação entre características biométricas, quanto à possibilidade de mudança na identificação, unicidade da identificação, grau de invasão da privacidade e dificuldade para cópia e roubo.

Tabela 9 – COMPARAÇÃO ENTRE AS CARACTERÍSTICAS BIOMÉTRICAS

Técnica de Reconhecimento	Mudança da Característica	Identificação Unívoca	Invasiva	Dificuldade para Cópia ou Roubo
Voz	Pouco provável	Média	Não	Baixa
Assinatura	Pouco provável	Média	Não	Média
Impressão digital	Pouco provável	Média	Não	Média
Face	Muito provável	Baixa	Não	Alta
Retina	Improvável	Alta	Sim	Impossível
Íris	Improvável	Alta	Sim	Impossível
Mapa de Veias	Pouco provável	Média	Não	Alta

Fonte: BASEADO EM JANES (2016) E PINHEIRO (2008)

Observa-se também na tabela 10, uma comparação entre as tecnologias biométricas, segundo o critério de padrão codificado, taxa de falhas na identificação, nível de segurança e aplicabilidade.

Tabela 10 – COMPARAÇÃO ENTRE AS TECNOLOGIAS BIOMÉTRICAS

Característica Biométrica	Padrão Codificado	Taxa de Falhas na Identificação	Nível de Segurança	Aplicabilidade
Reconhecimento da íris	Padrões da íris	1 em 1200000	Alto	Instalações de alta segurança
Impressão digital	Impressão digital	1 em 1000	Médio	Autenticação, controle de acesso e entre outros
Geometria da mão	Tamanho, comprimento, largura	1 em 700	Baixo	Instalações de baixa segurança
Reconhecimento facial	Perfil, distribuição dos pontos nodais	1 em 100	Baixo	Instalações de baixa segurança
Assinatura	Modo de escrita e pressão sob superfície	1 em 100	Baixo	Instalações de baixa segurança
Reconhecimento da voz	Características da voz	1 em 30	Baixo	Serviços de telefonia
Mapa de Veias	Mapeamento das veias da palma da mão	1 em 1000	Alto	Autenticação em operações bancárias e entre outros

Fonte: PINHEIRO (2008) E JANES (2016)

A fim de enfatizar mais sobre os tipos de biometria, a tabela 11, traz uma análise comparativa geral de várias destas tecnologias mais recentes, incluindo inclusive a tecnologia LFD para reconhecimento de impressão digital.

Tabela 11 – ANÁLISE COMPARATIVA GERAL DE TECNOLOGIAS BIOMÉTRICAS RECENTES

Tipo de Biométrica	Precisão	Custo	Tamanho Padrão	Nível de Segurança
Reconhecimento da íris e retina	Alto	Alto	Pequeno	Alto
Mapa de Veias	Alto	Médio	Médio	Alto
Reconhecimento facial	Baixo	Alto	Grande	Baixo
Reconhecimento da voz	Baixo	Médio	Pequeno	Baixo
Impressão digital (sem tecnologia LFD)	Baixo	Baixo	Pequeno	Baixo
Impressão digital (tecnologia LFD)	Médio	Baixo	Pequeno	Médio

Fonte: BASEADO EM ALEJO (2015), SUPREMA (2016) E FUTRONIC (2017)

Partindo do comparativo apresentados nas tabelas 9, 10 e 11, para o fator de autenticação “algo que você é” foi escolhido à técnica de reconhecimento por impressão digital, utilizado a tecnologia biométrica LFD, devido a mesma ter um custo baixo para desenvolvimento da aplicação, nível médio de segurança aceitável e por não ser invasivo.

Os fabricantes Suprema e Cis garantem que em seus leitores biométricos *finger scan* com tecnologia LFD, são providos contra autenticação com impressão digital falsa (*spoofing*).

A figura 51 apresenta diferentes técnicas para se gerar impressões digitais falsas e o desempenho de dispositivos para detectá-las. O sistema dos leitores BioStation A2 da Suprema e o FS 88H da empresa Cis, utilizado neste projeto, são um dos mais eficientes neste quesito, os quais possuem mesmo tipo de certificações, como por exemplo: FBI (norma PIV-071006).

Fake Finger	Material & Characteristic	Device A	Device B	BioStation A2
	Paper inversely printed	O	O	O
	Film inversely printed	O	O	O
	Glue	O	O	O
	Rubber	O	O	O
	Clay	X	O	O
	Silicone (Transparent)	X	X	O
	Silicone (Opaque)	X	X	O

Figura 51 – FAKE FINGER (SPOOFING)

Fonte: SUPREMA (2016)

Com relação ao tipo de *scanner* empregado para fazer a leitura da impressão digital, a tabela 12 traz um quadro comparativo das principais tecnologias empregadas.

Tabela 12 – COMPARAÇÃO ENTRE OS DISPOSITIVOS DE LEITORAS DE IMPRESSÃO DIGITAL

Tipo de *Scanner*	**Característica**
Capacitivo	Trabalha medindo o calor que sai da digital do dedo do indivíduo, para capturar as informações das minúcias.
Ótico	Trabalha emitindo uma luz sobre a digital do dedo do indivíduo. Quando esta luz é refletida o dispositivo consegue capturar as informações das minúcias. Este tipo de *scanner* é um dos sistemas mais seguros, no processo de leitura da impressão digital.
Ultrassônico	Trabalha emitindo sinais sonoros para analisar o retorno deles, capturando assim as informações das minúcias.

Fonte: TABELA RESUMIDA (BASEADO NO TÓPICO IMPRESSÃO DIGITAL)

Assim, levando-se em conta a qualidade da leitura de impressão digital, escolheu-se o tipo *scanner* ótico. Segundo Campos (2007), o *scanner* ótico é o mais utilizado atualmente nas

leitoras de impressões digitais e também é o mais seguro, pois mesmo que o dedo do usuário esteja sujo, o dispositivo ainda é capaz de capturar com sucesso as informações das minúcias.

Segundo Pinheiro (2008), ter apenas um bom *scanner* não é suficiente, pois é essencial ter um bom *software* para dar um tratamento adequado do sinal capturado (imagem capturada) para se fazer seu reconhecimento digital, com precisão. Estas imagens geram, em geral, arquivos de 256 a 669 bytes. Atualmente existem dois tipos de sistemas básicos, que utilizam estes dispositivos (leitoras), conforme a tabela 13:

Tabela 13 – COMPARAÇÃO ENTRE OS SISTEMAS DE RECONHECIMENTO DE IMPRESSÃO DIGITAL

Tipo de Software	Característica
Sistema de Impressão Latente	Neste sistema utiliza-se o dispositivo (leitora), para se capturar do indivíduo sua impressão digital. Em seguida, o arquivo gerado é enviado para um banco de dados central, localizado em servidores, geralmente distantes da forma colhedora, onde será feito a comparação da mesma com outras impressões digitais. Este procedimento torna a aplicação lenta.
Sistema em Tempo Real	Neste sistema utiliza-se o dispositivo (leitora), para capturar a impressão digital do indivíduo, processar e comparar a mesma com outras impressões digitais, as quais já estão armazenadas em seu banco de dados local, a que torna a aplicação deste sistema mais rápido, em comparação com sistema de impressão latente.

Fonte: TABELA RESUMIDA (BASEADO NO TÓPICO 2.4.1)

Sendo assim, baseado na análise dos modelos de reconhecimento de impressão apresentados na tabela 13, escolheu-se o *software* em sistema de tempo real, o qual fará os procedimentos de captura, processamento e comparação da impressão digital, com aquelas já armazenadas no próprio *java card* (certificado tipo A3). Com isso, a aplicação do *software* de emissão de NF-e do emitente (empresa), funciona de forma mais rápida.

Diante dos fatos apresentados anteriormente, para o fator de autenticação “algo que você é” foi escolhido à tecnologia de biometria por reconhecimento de impressão digital (tecnologia LFD), pelo mesmo prover: o princípio de não-repúdio (impressões digitais são únicas para cada indivíduo, tendo-se conotação criminal nos EUA, Europa e na América Latina), baixo custo de

implantação, nível de segurança médio, dificuldade média para cópia ou roubo, confiabilidade (durante o ciclo de vida do usuário as características das digitais dos dedos são pouco prováveis de mudar), menos invasiva (muito bem aceito pelos usuários), nível de precisão médio, algoritmo avançado contra autenticação com impressão digital falsa (*spoofing*), taxa de falha durante a identificação de usuário de 1 em 1000 e por seu *template* ocupar de 256 a 669 bytes, o qual pode ser armazenado facilmente em um *smart card*, mais especificamente no *java card* J2A080 que iremos utilizar no projeto.

5.3 APRESENTAÇÃO DA SOLUÇÃO

Neste projeto foram utilizados dois fatores para o processo de assinatura digital da NF-e, baseados em autenticação por *hardware*, justificados acima: *java card* e o leitor biométrico por reconhecimento de impressão digital, utilizando a tecnologia LFD. Na solução sugerida são necessários quatro módulos de sistemas, que atendem as normas do projeto da NF-e (ENCAT, 2015) e dos padrões da ISO 7816 e VISA:

1. Módulo de instalação do arquivo *.cap no *java card* – É responsável por visualizar os applet's, existentes no *java card*, bem como tem a função de realizar download do arquivo *.cap e instalá-los dentro do mesmo. Para realizar estas tarefas foi utilizado o PyApduTool do JC kit, como ambiente de simulação para uma unidade certificadora (CA), conforme figura 52;
2. Módulo de configuração do cartão biométrico – Sua função é de fazer todo o processo de cadastramento do PIN biométrico, geração das chaves simétricas (atrelado e único para cada *java card* e aplicação cliente) e também dos três pares de chaves assimétrico (privada e pública), de acordo com o padrão VISA;
3. Módulo de assinatura digital da NF-e – Este módulo foi desenvolvido para o ambiente de simulação utilizada, e tem como função permitir que os usuários escolham o arquivo XML, o assina, para que seja possível a geração da NF-e, de acordo com os padrões estabelecidos do ENCAT (2016), poder visualizá-la, bem como, validá-la;
4. Módulo de verificação da assinatura digital e da NF-e – Permite a simulação de uma AC e também de um servidor da SEFAZ. Sua função é a de verificar a autenticidade e integridade, da assinatura digital, bem como, todo o conteúdo do arquivo XML da NF-e.

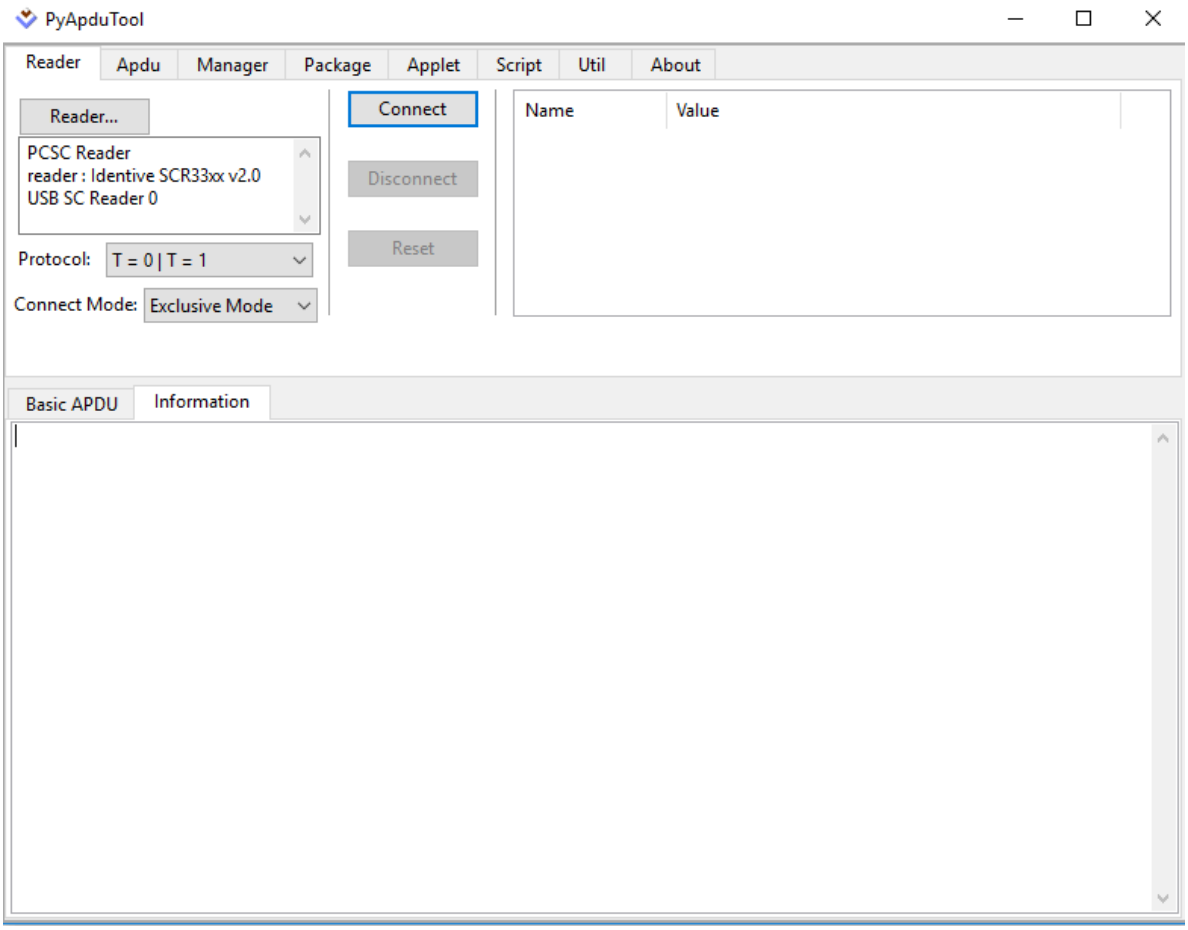


Figura 52 – PYAPDUTOOL DO JC KIT
Fonte: FIGURA REALIZADA PELO AUTOR

O módulo de configuração do cartão biométrico é composto por quatro etapas, conforme fluxo apresentado na figura 53:

1. Coleta do *template* biométrico;
2. Coleta do PUK, geração de chave simétricas e também dos três pares de chaves assimétrico (privada e pública) e o certificado da autoridade certificadora (CA), de acordo com o padrão VISA;
3. Gravação do cartão;
4. Teste do cartão.

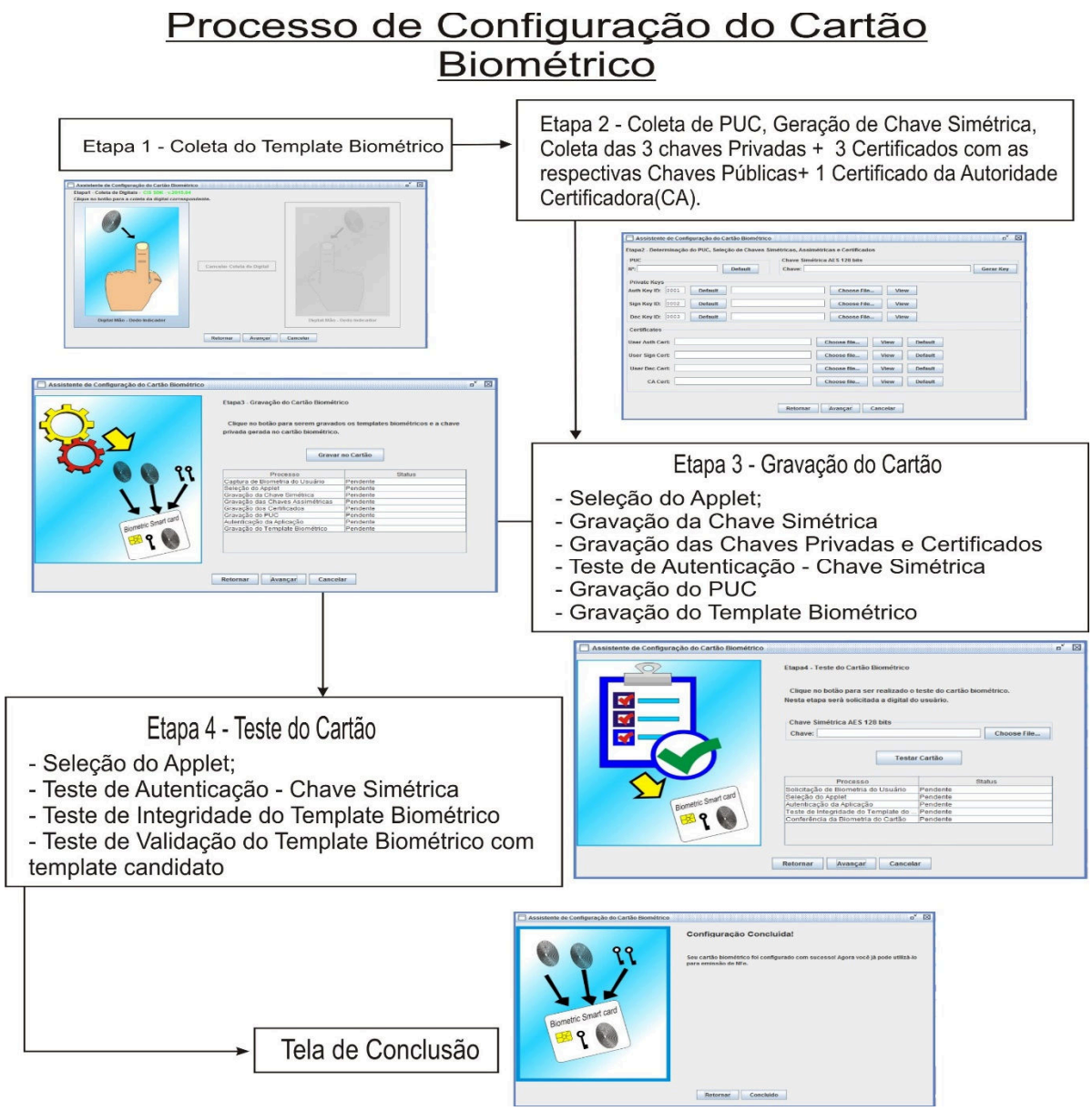


Figura 53 – PROCESSO DE CONFIGURAÇÃO DO CARTÃO BIOMÉTRICO

Fonte: FIGURA REALIZADA PELO AUTOR

Ainda na etapa 2 do processo de configuração referente a gravação das chaves simétrica e assimétrica, PUK, certificados da unidade certificado (CA), para dentro do *java card*, foram utilizados exemplos fornecidos pelo projeto *open source* (PKIApplet).

Ainda na figura 53, enfatiza-se que na etapa 2, a unidade certificadora (CA) é responsável por emitir um par de chave simétrico (CBC) e único, para cada *java card* (PKIApplet) e com sua respectiva aplicação cliente (PKIHostAPI). Se faz necessário tal procedimento para que o *java card* (PKIApplet) forneça somente o *template* biométrico para aplicação cliente (PKIHostAPI) legítima, evitando assim que o atacante possa capturar o mesmo e também evita o tipo de ataque (*padding oracle*), pois a implementação do código fonte do projeto *open source*

PKIApplet, o *applet* (servidor) que está dentro *java card* não responde livremente a consultas de qualquer host ou aplicações ilícitas, por isso utiliza-se o método *get challenger* e a função de autenticação externa que está descrito na figura 54.

Na etapa 3, na figura 53, é realizado um *select* do AID do *applet* (servidor), para realizar todas as gravações das: chave simétrica, chaves assimétricas e certificado, para que posteriormente seja efetuado um teste de autenticação da chave simétrica. Se todas as gravações forem concluídas no *java card*, então será gravado agora o PUK.

Por fim, na etapa 4 da figura 53, é realizado o teste do *java card*. Para ser feito o teste, primeiro o usuário deve informar onde é que está a chave simétrica. É solicitado ao usuário que apresente sua digital. Após isto, é realizado um *select* do AID do *applet* (servidor), para realizar a autenticação externa, que permitirá solicitação do *template* biométrico de referência, a fim de ser realizado o teste de integridade deste *template*.

O processo de autenticação externa, que é melhor explicitado na figura 54, visa autenticar a aplicação cliente (*host*) ao *java card*. Para que aplicação tenha permissão de acesso ao *template* de referência. Este protocolo de comunicação começa com a solicitação do desafio da aplicação ao *java card*, através de um método *get challenger*. O *java card* no método *get challenger* gera um código de desafio "R" e o envia a aplicação cliente (*host*). A aplicação recebe o código de desafio, o criptografa, utilizando chave simétrica. Após este procedimento, a aplicação envia o comando de autenticação externa com o código encriptado "E(R) ".

O *java card* de autenticação externa recebe o código encriptado "E(R)", e o descriptografa, utilizando a mesma chave simétrica "D(E(R))", finalmente compara o resultado com o valor "R" gerado pelo método *get challenger*.

Se D(E(R))" = "R" o desafio foi resolvido, e a aplicação está autenticada com o *java card*. Neste momento é ativada uma variável de autenticação no *java card*, a qual permite a solicitação do *template* biométrico de referência.

No teste de integridade o *template* de referência que foi recebido do *java card*, é comparado com o *template* coletado na etapa 2, da figura 53, afim de verificar sua integridade. Vale lembrar que quando o java card envia o *template* de referência, é gerado um código de verificação que será utilizado para indicar ao *java card* que o teste de comparação entre o *template* de referência e o *template* candidato ocorreu com sucesso. Após esta verificação é feita a comparação entre o *template* de referência e o candidato. Caso os *templates* coincidam, deve ser enviado o código de verificação encriptado com a chave simétrica para o *java card*, a fim de indicar que o processo ocorreu com sucesso.

Ocorrendo com sucesso é ativado no *template* o atributo *valid* para *true*, indicando que o *template* foi validado: a variável *remaningattemps* é reinicializada com o valor *trylimit* do *template*. Se não ocorrer com sucesso o atributo *valid* do *template* é indicado como *false*, e a variável *remaningattemps* o decrementa. Caso a variável *remaningattemps* atinja o valor zero, o *java card* é bloqueado. Caso o *java card* não esteja bloqueado, é exibida a mensagem de que a digital apresentada não confere, assim como, a quantidade restante de tentativas.

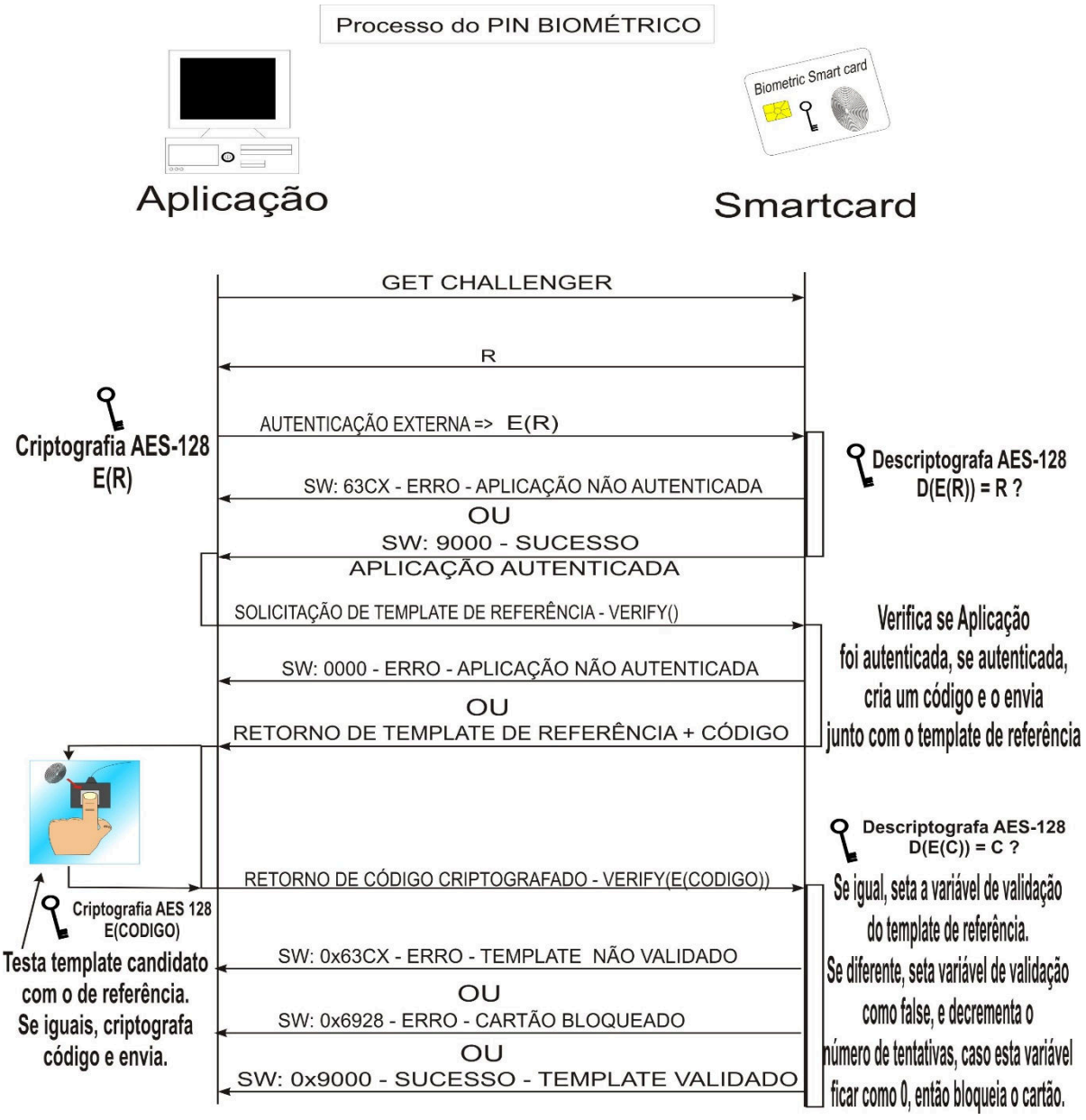


Figura 54 – PROTOCOLO DE COMUNICAÇÃO (AUTENTICAÇÃO EXTERNA)

Fonte: FIGURA REALIZADA PELO AUTOR

Por fim, no módulo de assinatura digital da NF-e, foi implementada uma aplicação que funciona de acordo com todos os requisitos do projeto da NF-e (ENCAT, 2015), as normas da ISO 7816 e o padrão VISA, para que os participantes possam assinar um arquivo XML e emitir uma NF-e, em um ambiente de simulação de nosso experimento, similar a um emissor homologado pela SEFAZ. As figuras 55 e 56 mostram respectivamente: os equipamentos (módulos de *hardware*) envolvidos no projeto e a tela do assistente de assinatura da NF-e.

Figura 55 – EQUIPAMENTOS DE HARDWARE ENVOLVIDOS
Fonte: FIGURA REALIZADA PELO AUTOR

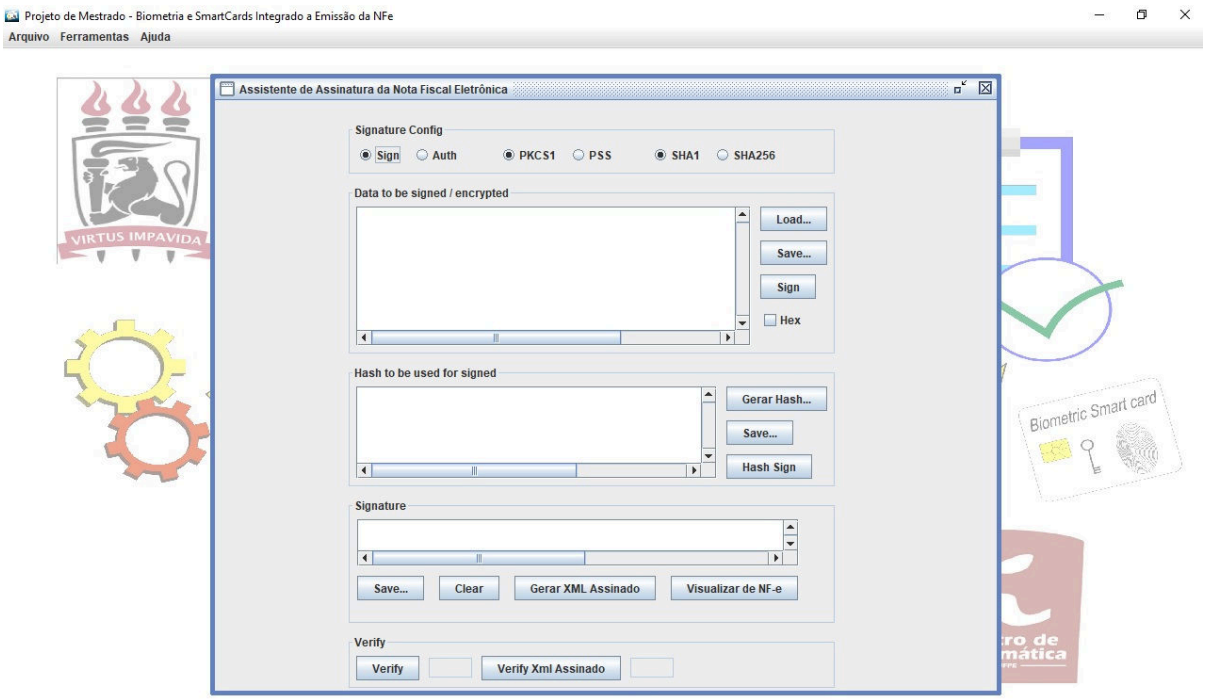


Figura 56 – ASSISTENTE DE ASSINATURA DA NOTA FISCAL ELETRÔNICA
Fonte: FIGURA REALIZADA PELO AUTOR

A tela inicial do assistente de assinatura da nota fiscal eletrônica, pertencente ao módulo de assinatura digital da NF-e, conforme figura 57, pode ser descrita em quatro etapas. Para

facilitar a simulação do ambiente foram escolhidos como padrão as opções *Sign*, *PKCS1* e *SHA1*, que são padrão de assinatura do projeto da NF-e (ENCAT, 2015):

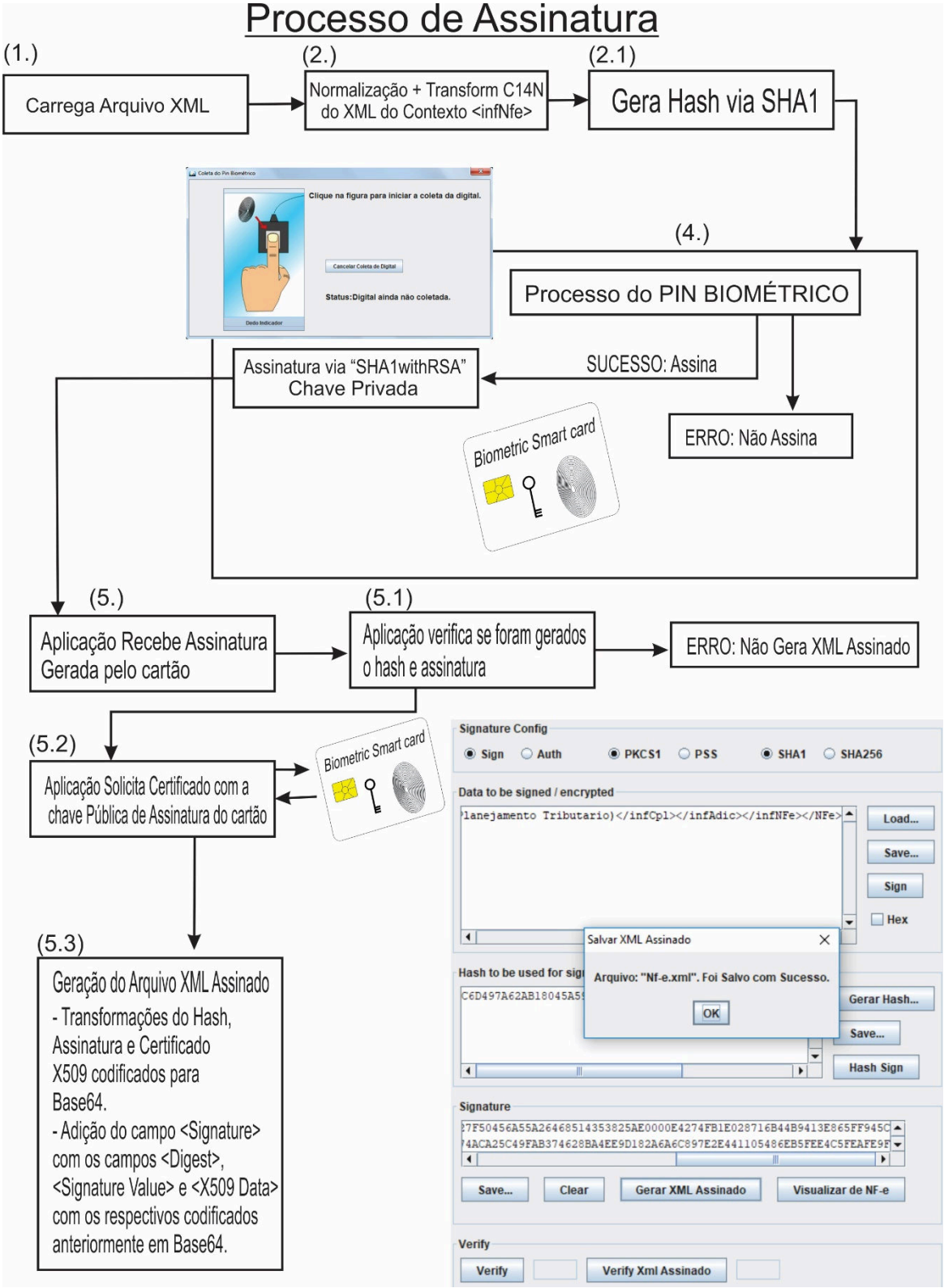


Figura 57 – PROCESSO DE ASSINATURA

Fonte: FIGURA REALIZADA PELO AUTOR

Etapas da simulação:

1. O usuário através do botão "*Load*", carrega o arquivo XML e o apresenta no campo indicado. Vale lembrar que foi utilizado um arquivo XML, conforme apêndice C, de acordo com o *schema* vigente da NF-e, para posteriormente ser assinado. O arquivo XML mencionado foi criado através do XStream;
2. Agora, através do botão "Gerar *hash*" é selecionado o contexto de assinatura, o qual é o conteúdo da *tag* infNFe. Em seguida é realizada a normalização do contexto, feita a canonização C14N e a geração do *hash*;
3. Após a geração do *hash*, o mesmo é exibido na tela em formato *base64*;
4. Deve-se gerar então a assinatura do XML, utilizando o valor do *hash*, através do botão "*Hash Sign*". Neste momento é solicitado o PIN biométrico e lançado novamente a autenticação externa mencionada na figura 54, para posteriormente ser exibido na tela o valor da assinatura no formato *base64*, conforme figura 58. Caso ocorra erro na validação, é retornado uma mensagem de erro e não se realiza a assinatura do XML da NF-e;

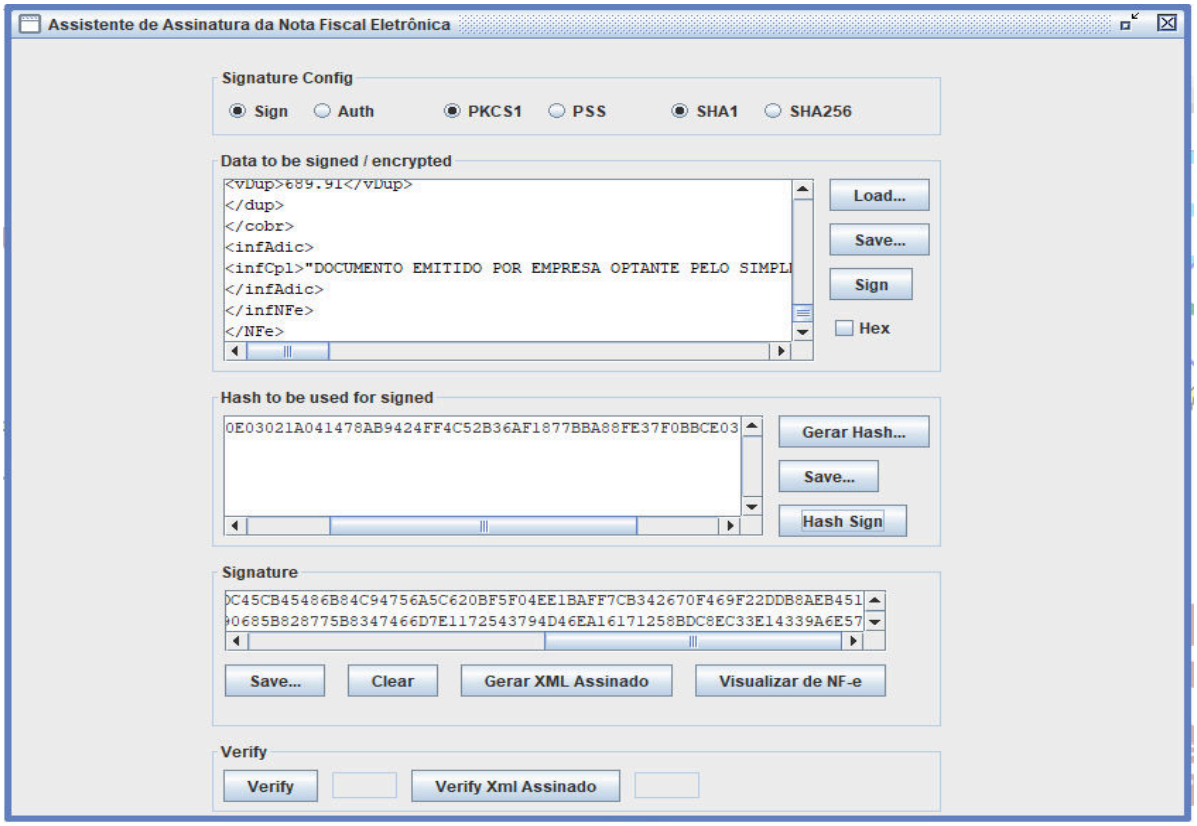


Figura 58 – VALOR DA ASSINATURA DIGITAL (BASE64)

Fonte: FIGURA REALIZADA PELO AUTOR

5. Se não ocorreu erro emite-se uma NF-e, através do botão “Gerar XML Assinado”, a qual será anexado no arquivo XML. Depois da *tag* infNFe, uma nova *tag* chamada *Signature* é gerada, contendo os valores do *hash*, assinatura digital e o certificado digital, todos convertidos em *base64*. No projeto foi simulado a situação onde o servidor da SEFAZ, faz a validação do *schema* das *tag's*, do arquivo XML, antes de informar: chave de acesso na *tag* infNFe, protocolo de autorização de uso na *tag* nProt e com horário da autorização na *tag* dhRecbto, para posteriormente ser anexado no XML assinado da NF-e;
6. Após o processo de assinatura digital da NF-e e posterior emissão da NF-e, o usuário pode visualizar a mesma, no aplicativo através do botão “Visualizador do DANFE”;
7. Ao abrir o programa Visualizador de XML (NFe/Cte/NFCe), conforme figura 59, o usuário pode selecionar o XML assinado, referente ao DANFE, e com isso visualizar a mesma, dentro do padrão de leiaute do manual de orientação do contribuinte (ENCAT, 2015). O usuário tem a opção de imprimir o DANFE da NF-e, conforme figura 60. Caso a arquivo XML da NF-e não esteja assinada, apresenta-se a visualização do DANFE como NF-e não enviada para SEFAZ, conforme figura 61.

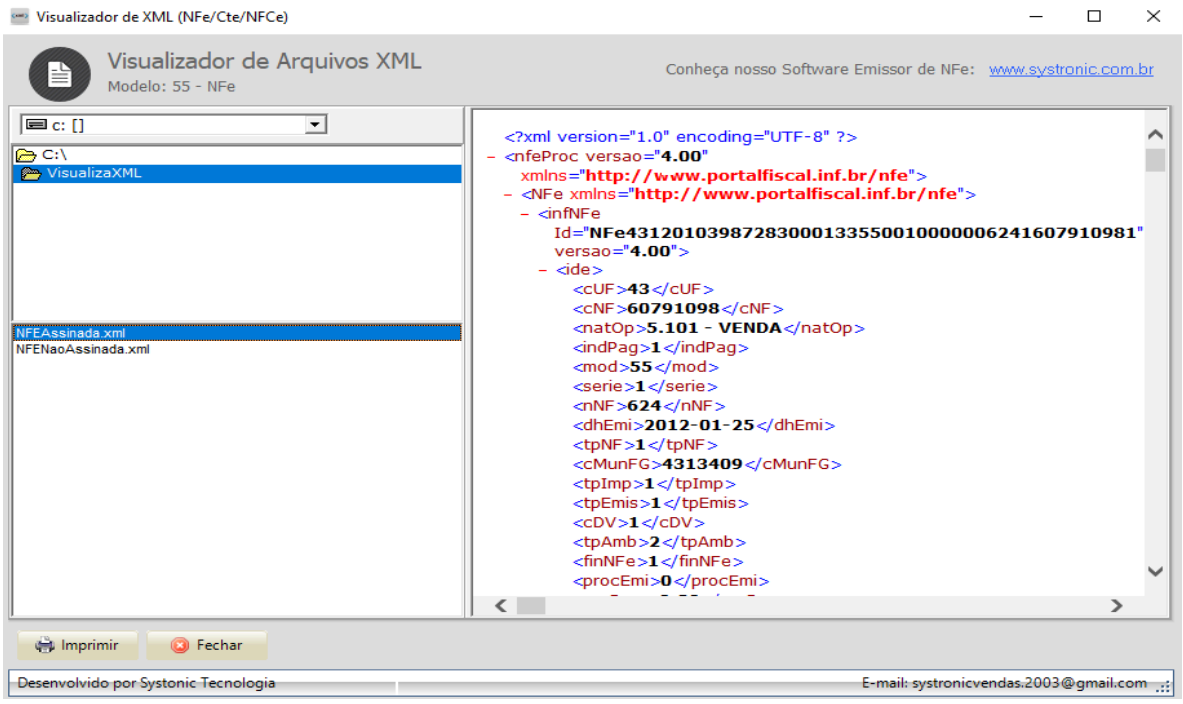
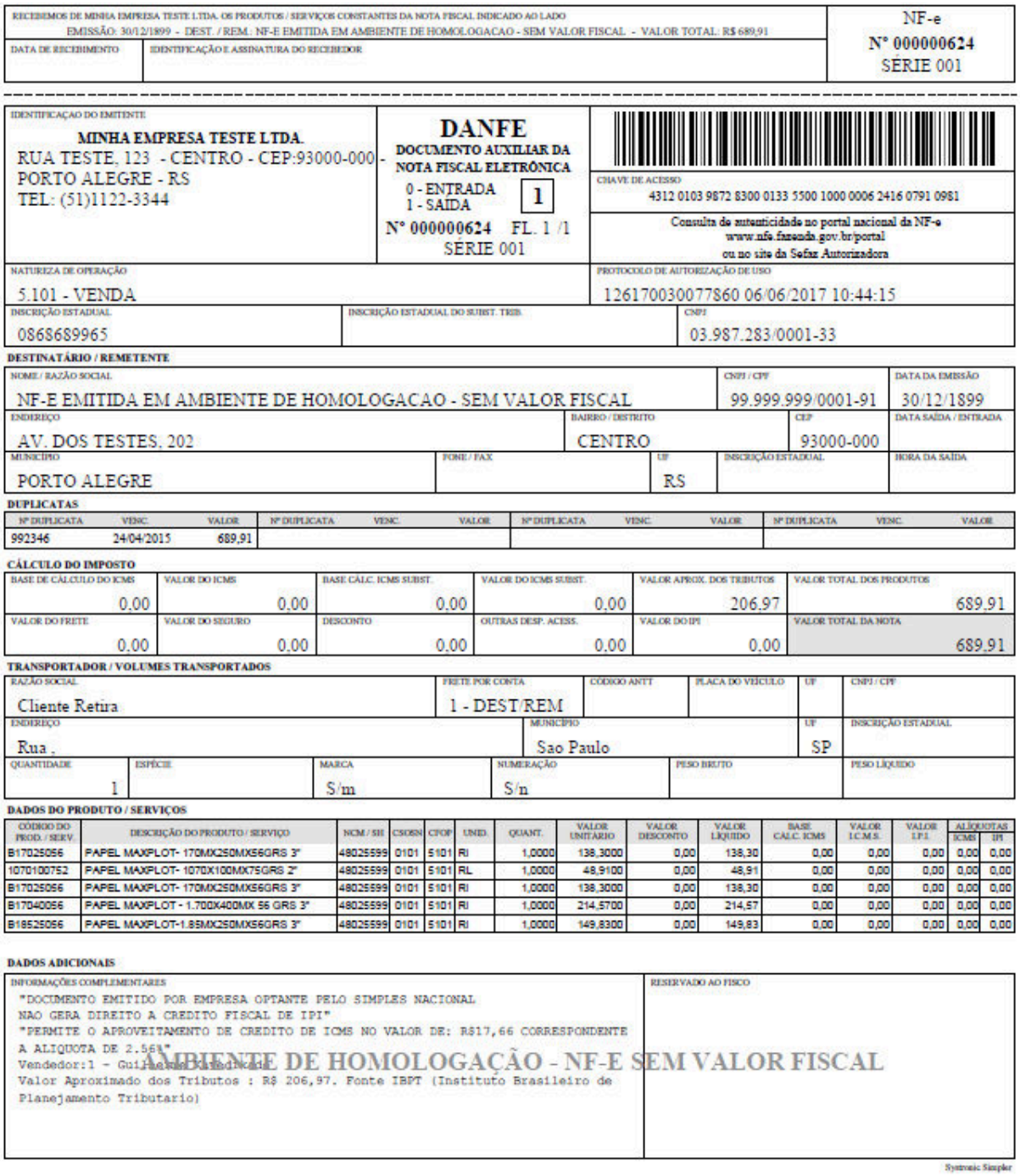


Figura 59 – VISUALIZADOR DE XML (NFE/CTE/NFCE)

Fonte: SYSTONIC TECNOLOGIA (2017)



RECEBEMOS DE MINHA EMPRESA TESTE LTDA. OS PRODUTOS / SERVIÇOS CONSTANTES DA NOTA FISCAL INDICADO AO LADO
EMISSÃO: 30/12/1899 - DEST. / REM.: NF-E EMITIDA EM AMBIENTE DE HOMOLOGACAO - SEM VALOR FISCAL - VALOR TOTAL: R$ 689,91

DATA DE RECEBIMENTO	IDENTIFICAÇÃO E ASSINATURA DO RECEBEDOR

NF-e
N° 000000624
SÉRIE 001

IDENTIFICAÇÃO DO EMITENTE
MINHA EMPRESA TESTE LTDA.
RUA TESTE, 123 - CENTRO - CEP:93000-000 -
PORTO ALEGRE - RS
TEL: (51)1122-3344

DANFE
DOCUMENTO AUXILIAR DA NOTA FISCAL ELETRÔNICA
0 - ENTRADA
1 - SAÍDA [1]
N° 000000624 FL. 1 /1
SÉRIE 001

CHAVE DE ACESSO
4312 0103 9872 8300 0133 5500 1000 0006 2416 0791 0981

Consulta de autenticidade no portal nacional da NF-e
www.nfe.fazenda.gov.br/portal
ou no site da Sefaz Autorizadora

NATUREZA DE OPERAÇÃO	PROTOCOLO DE AUTORIZAÇÃO DE USO
5.101 - VENDA	126170030077860 06/06/2017 10:44:15

INSCRIÇÃO ESTADUAL	INSCRIÇÃO ESTADUAL DO SUBST. TRIB.	CNPJ
0868689965		03.987.283/0001-33

DESTINATÁRIO / REMETENTE

NOME / RAZÃO SOCIAL			CNPJ / CPF	DATA DA EMISSÃO
NF-E EMITIDA EM AMBIENTE DE HOMOLOGACAO - SEM VALOR FISCAL			99.999.999/0001-91	30/12/1899
ENDEREÇO	**BAIRRO / DISTRITO**		**CEP**	**DATA SAÍDA / ENTRADA**
AV. DOS TESTES, 202	CENTRO		93000-000	
MUNICÍPIO	**FONE / FAX**	**UF**	**INSCRIÇÃO ESTADUAL**	**HORA DA SAÍDA**
PORTO ALEGRE		RS		

DUPLICATAS

Nº DUPLICATA	VENC.	VALOR	Nº DUPLICATA	VENC.	VALOR	Nº DUPLICATA	VENC.	VALOR	Nº DUPLICATA	VENC.	VALOR
992346	24/04/2015	689,91									

CÁLCULO DO IMPOSTO

BASE DE CÁLCULO DO ICMS	VALOR DO ICMS	BASE CÁLC. ICMS SUBST.	VALOR DO ICMS SUBST.	VALOR APROX. DOS TRIBUTOS	VALOR TOTAL DOS PRODUTOS
0,00	0,00	0,00	0,00	206,97	689,91
VALOR DO FRETE	**VALOR DO SEGURO**	**DESCONTO**	**OUTRAS DESP. ACESS.**	**VALOR DO IPI**	**VALOR TOTAL DA NOTA**
0,00	0,00	0,00	0,00	0,00	689,91

TRANSPORTADOR / VOLUMES TRANSPORTADOS

RAZÃO SOCIAL	FRETE POR CONTA	CÓDIGO ANTT	PLACA DO VEÍCULO	UF	CNPJ / CPF
Cliente Retira	1 - DEST/REM				
ENDEREÇO	**MUNICÍPIO**			**UF**	**INSCRIÇÃO ESTADUAL**
Rua ,	Sao Paulo			SP	

QUANTIDADE	ESPÉCIE	MARCA	NUMERAÇÃO	PESO BRUTO	PESO LÍQUIDO
1		S/m	S/n		

DADOS DO PRODUTO / SERVIÇOS

CÓDIGO DO PROD. / SERV.	DESCRIÇÃO DO PRODUTO / SERVIÇO	NCM / SH	CSOSN	CFOP	UNID.	QUANT.	VALOR UNITÁRIO	VALOR DESCONTO	VALOR LÍQUIDO	BASE CÁLC. ICMS	VALOR I.C.M.S.	VALOR I.P.I.	ALÍQUOTAS ICMS	ALÍQUOTAS IPI
B17025056	PAPEL MAXPLOT- 170MX25OMX56GRS 3"	48025599	0101	5101	RI	1,0000	138,3000	0,00	138,30	0,00	0,00	0,00	0,00	0,00
1070100752	PAPEL MAXPLOT- 1070X100MX75GRS 2"	48025599	0101	5101	RL	1,0000	48,9100	0,00	48,91	0,00	0,00	0,00	0,00	0,00
B17025056	PAPEL MAXPLOT- 170MX25OMX56GRS 3"	48025599	0101	5101	RI	1,0000	138,3000	0,00	138,30	0,00	0,00	0,00	0,00	0,00
B17040056	PAPEL MAXPLOT - 1.700X400MX 56 GRS 3"	48025599	0101	5101	RI	1,0000	214,5700	0,00	214,57	0,00	0,00	0,00	0,00	0,00
B18525056	PAPEL MAXPLOT-1.85MX25OMX56GRS 3"	48025599	0101	5101	RI	1,0000	149,8300	0,00	149,83	0,00	0,00	0,00	0,00	0,00

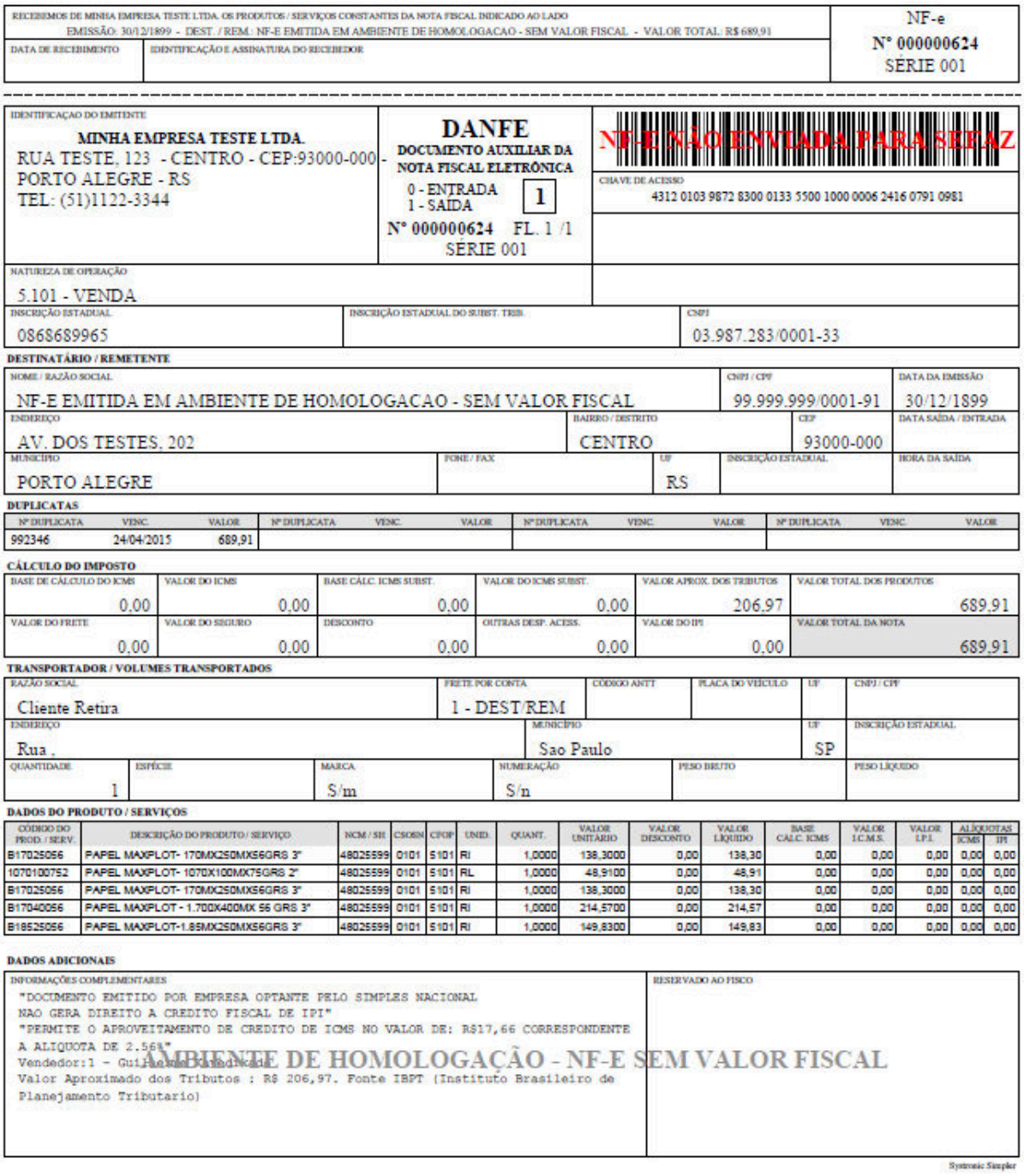
DADOS ADICIONAIS

INFORMAÇÕES COMPLEMENTARES	RESERVADO AO FISCO
"DOCUMENTO EMITIDO POR EMPRESA OPTANTE PELO SIMPLES NACIONAL NAO GERA DIREITO A CREDITO FISCAL DE IPI" "PERMITE O APROVEITAMENTO DE CREDITO DE ICMS NO VALOR DE: R$17,66 CORRESPONDENTE A ALIQUOTA DE 2.56%" Vendedor:1 - Guilherme Bittencourt Valor Aproximado dos Tributos : R$ 206,97. Fonte IBPT (Instituto Brasileiro de Planejamento Tributario)	AMBIENTE DE HOMOLOGAÇÃO - NF-E SEM VALOR FISCAL

Systemic Simpler

Figura 60 – NF-e ASSINADA E AUTORIZADA PELA SEFAZ

Fonte: FIGURA REALIZADA PELO AUTOR



RECEBEMOS DE MINHA EMPRESA TESTE LTDA. OS PRODUTOS / SERVIÇOS CONSTANTES DA NOTA FISCAL INDICADO AO LADO
EMISSÃO: 30/12/1899 - DEST. / REM.: NF-E EMITIDA EM AMBIENTE DE HOMOLOGACAO - SEM VALOR FISCAL - VALOR TOTAL: R$ 689,91

DATA DE RECEBIMENTO	IDENTIFICAÇÃO E ASSINATURA DO RECEBEDOR

NF-e
N° 000000624
SÉRIE 001

IDENTIFICAÇÃO DO EMITENTE
MINHA EMPRESA TESTE LTDA.
RUA TESTE, 123 - CENTRO - CEP:93000-000
PORTO ALEGRE - RS
TEL: (51)1122-3344

DANFE
DOCUMENTO AUXILIAR DA NOTA FISCAL ELETRÔNICA
0 - ENTRADA
1 - SAÍDA [1]
N° 000000624 FL. 1 /1
SÉRIE 001

NF-E NÃO ENVIADA PARA SEFAZ

CHAVE DE ACESSO
4312 0103 9872 8300 0133 5500 1000 0006 2416 0791 0981

NATUREZA DE OPERAÇÃO		
5.101 - VENDA		
INSCRIÇÃO ESTADUAL	**INSCRIÇÃO ESTADUAL DO SUBST. TRIB.**	**CNPJ**
0868689965		03.987.283/0001-33

DESTINATÁRIO / REMETENTE

NOME / RAZÃO SOCIAL			CNPJ / CPF	DATA DA EMISSÃO
NF-E EMITIDA EM AMBIENTE DE HOMOLOGACAO - SEM VALOR FISCAL			99.999.999/0001-91	30/12/1899
ENDEREÇO	**BAIRRO / DISTRITO**		**CEP**	**DATA SAÍDA / ENTRADA**
AV. DOS TESTES, 202	CENTRO		93000-000	
MUNICÍPIO	**FONE / FAX**	**UF**	**INSCRIÇÃO ESTADUAL**	**HORA DA SAÍDA**
PORTO ALEGRE		RS		

DUPLICATAS

Nº DUPLICATA	VENC.	VALOR	Nº DUPLICATA	VENC.	VALOR	Nº DUPLICATA	VENC.	VALOR	Nº DUPLICATA	VENC.	VALOR
992346	24/04/2015	689,91									

CÁLCULO DO IMPOSTO

BASE DE CÁLCULO DO ICMS	VALOR DO ICMS	BASE CÁLC. ICMS SUBST.	VALOR DO ICMS SUBST.	VALOR APROX. DOS TRIBUTOS	VALOR TOTAL DOS PRODUTOS
0,00	0,00	0,00	0,00	206,97	689,91
VALOR DO FRETE	**VALOR DO SEGURO**	**DESCONTO**	**OUTRAS DESP. ACESS.**	**VALOR DO IPI**	**VALOR TOTAL DA NOTA**
0,00	0,00	0,00	0,00	0,00	689,91

TRANSPORTADOR / VOLUMES TRANSPORTADOS

RAZÃO SOCIAL	FRETE POR CONTA	CÓDIGO ANTT	PLACA DO VEÍCULO	UF	CNPJ / CPF
Cliente Retira	1 - DEST/REM				
ENDEREÇO	**MUNICÍPIO**			**UF**	**INSCRIÇÃO ESTADUAL**
Rua ,	Sao Paulo			SP	
QUANTIDADE	**ESPÉCIE**	**MARCA**	**NUMERAÇÃO**	**PESO BRUTO**	**PESO LÍQUIDO**
1		S/m	S/n		

DADOS DO PRODUTO / SERVIÇOS

CÓDIGO DO PROD. / SERV.	DESCRIÇÃO DO PRODUTO / SERVIÇO	NCM / SH	CSOSN	CFOP	UNID.	QUANT.	VALOR UNITÁRIO	VALOR DESCONTO	VALOR LÍQUIDO	BASE CÁLC. ICMS	VALOR I.C.M.S.	VALOR I.P.I.	ALÍQUOTAS ICMS	ALÍQUOTAS IPI
B17025056	PAPEL MAXPLOT- 170MX250MX56GRS 3"	48025599	0101	5101	RI	1,0000	138,3000	0,00	138,30	0,00	0,00	0,00	0,00	0,00
1070100752	PAPEL MAXPLOT- 1070X100MX75GRS 2"	48025599	0101	5101	RL	1,0000	48,9100	0,00	48,91	0,00	0,00	0,00	0,00	0,00
B17025056	PAPEL MAXPLOT- 170MX250MX56GRS 3"	48025599	0101	5101	RI	1,0000	138,3000	0,00	138,30	0,00	0,00	0,00	0,00	0,00
B17040056	PAPEL MAXPLOT - 1.700X400MX 56 GRS 3"	48025599	0101	5101	RI	1,0000	214,5700	0,00	214,57	0,00	0,00	0,00	0,00	0,00
B18525056	PAPEL MAXPLOT-1.85MX250MX56GRS 3"	48025599	0101	5101	RI	1,0000	149,8300	0,00	149,83	0,00	0,00	0,00	0,00	0,00

DADOS ADICIONAIS

INFORMAÇÕES COMPLEMENTARES	RESERVADO AO FISCO
"DOCUMENTO EMITIDO POR EMPRESA OPTANTE PELO SIMPLES NACIONAL NAO GERA DIREITO A CREDITO FISCAL DE IPI" "PERMITE O APROVEITAMENTO DE CREDITO DE ICMS NO VALOR DE: R$17,66 CORRESPONDENTE A ALIQUOTA DE 2.56%" Vendedor:1 - Guilherme Bandeira Valor Aproximado dos Tributos : R$ 206,97. Fonte IBPT (Instituto Brasileiro de Planejamento Tributario)	

AMBIENTE DE HOMOLOGAÇÃO - NF-E SEM VALOR FISCAL

Syntronic Simpler

Figura 61 – NF-e NÃO ENVIADA PARA SEFAZ
Fonte: FIGURA REALIZADA PELO AUTOR

Por fim, os módulos de verificação da assinatura digital e da NF-e, são totalmente funcionais e emulam um ambiente real de validação da AC e também da SEFAZ.

No aplicativo o botão "*Verify*", permite a verificação da autenticidade da assinatura digital do usuário, pela AC, através de seu certificado digital contido dentro do *java card*, conforme as figuras 58 e 62.

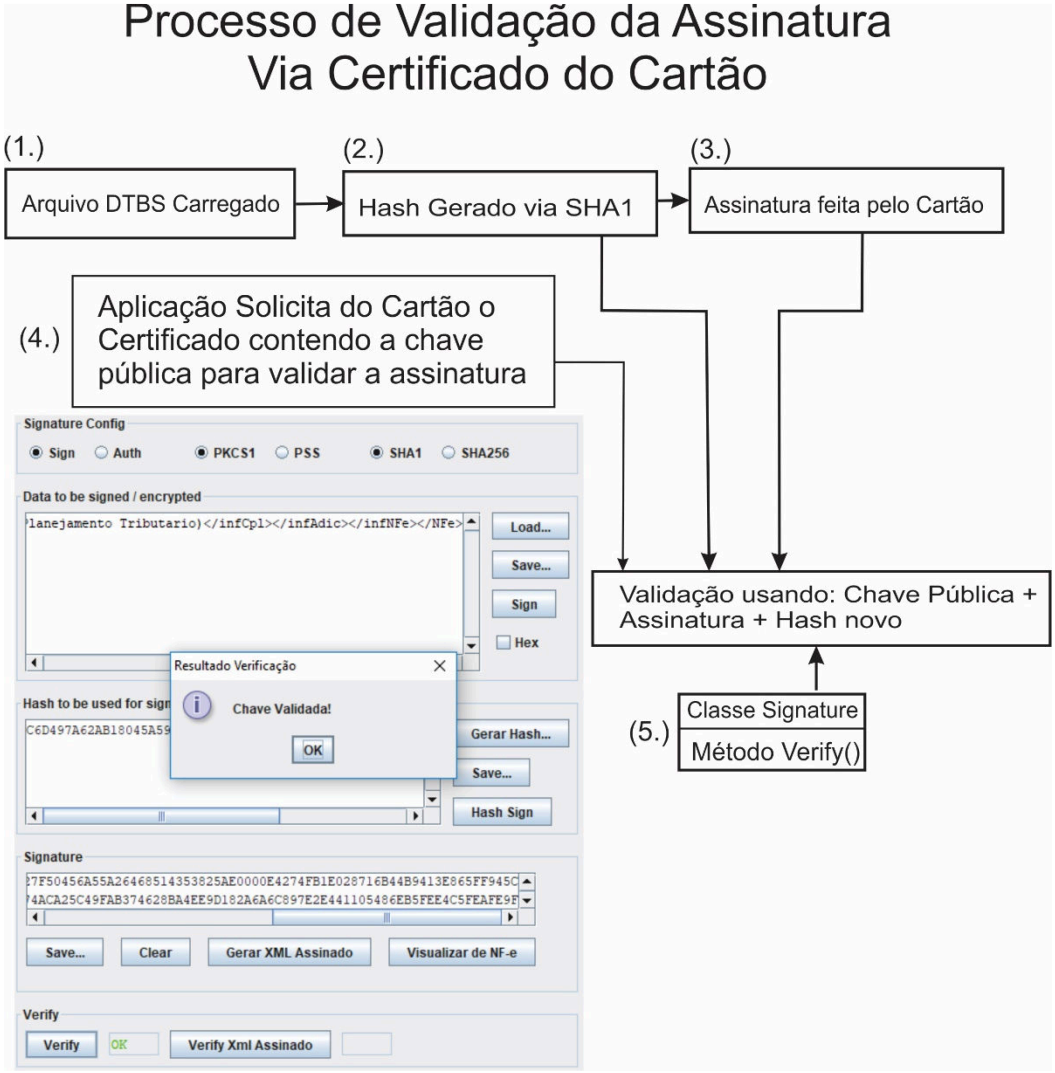


Figura 62 – PROCESSO DE VALIDAÇÃO DA ASSINATURA (JAVA CARD)

Fonte: FIGURA REALIZADA PELO AUTOR

A figura 62 apresenta o fluxo do processo de validação da assinatura digital do *java card*. O processo de validação é composto das seguintes etapas:

1. Carrega-se o arquivo DTBS (blocos de bit's), contendo os dados apresentados da tela, conforme exemplo da figura 58;
2. Gera-se um novo *hash* via SHA1 do arquivo DTBS e o envia para a classe *Signature*;
3. Captura a assinatura feita pelo cartão e a envia para a classe *Signature*;
4. Agora a aplicação solicita do *java card*, o certificado a chave púbica de validação e depois a envia para a classe *Signature*;
5. Por fim o método *Verify*(), da classe *Signature*, recebe todos os parâmetros necessário, para efetuar a comparação e apresentar a mensagem validação com

sucesso ou não. Com isso é possível garantir o princípio de autenticidade da assinatura digital do mesmo, de acordo com conceitos da PSI.

Ainda no módulo de verificação da assinatura digital e da NF-e, procura-se demonstrar que o aplicativo, além de ser funcional para AC, também pode ser utilizado em um ambiente real pela SEFAZ, para fins de validação do XML assinado da NF-e. Se for acionado o botão "*Verify* XML Assinado", a aplicação verifica a autenticidade da assinatura digital do usuário, bem como, a integridade dos dados contidos na NF-e.

O processo de validação da assinatura em XML, pode ser visto no fluxo apresentado na figura 63.

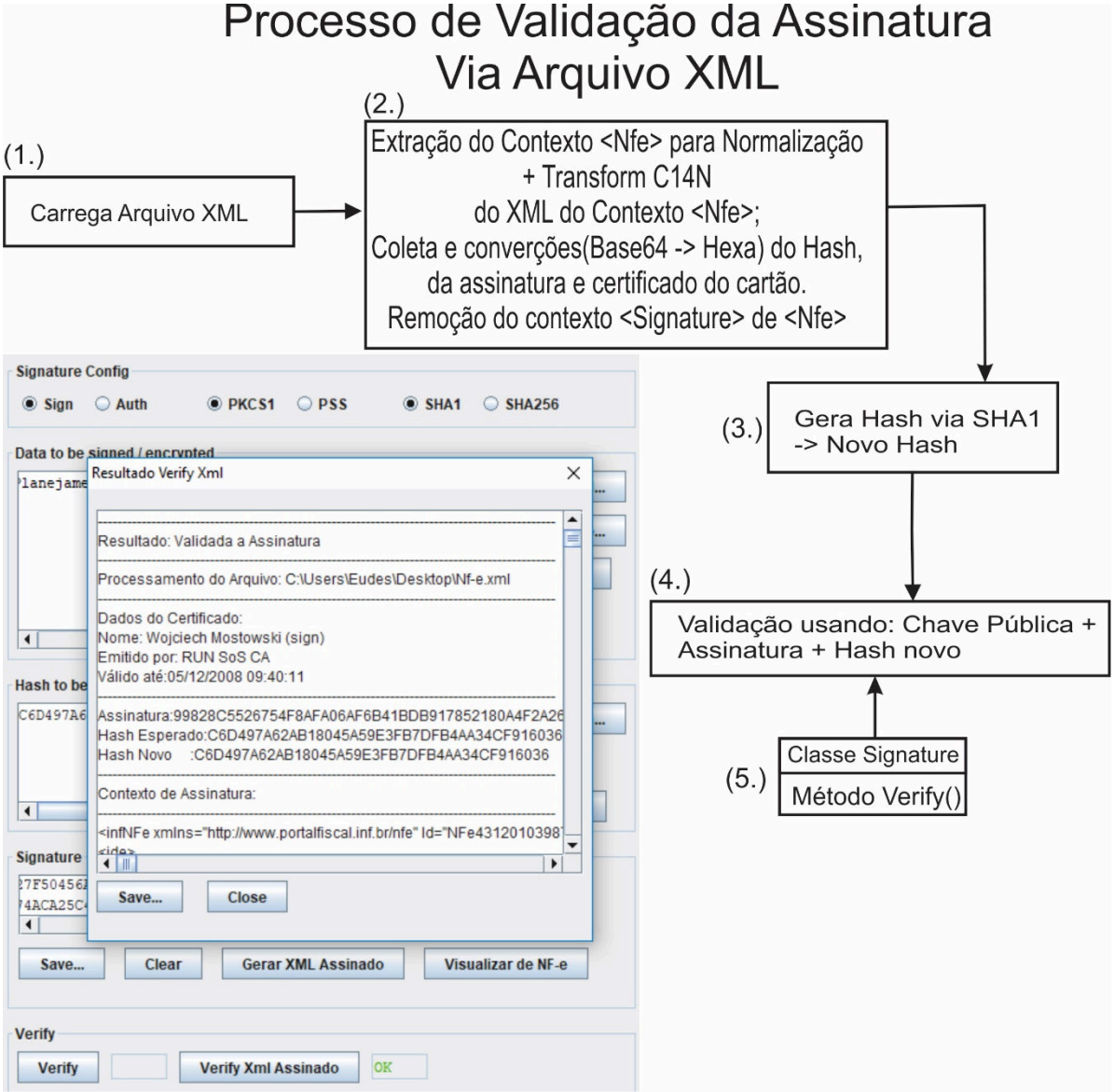


Figura 63 – PROCESSO DE VALIDAÇÃO DA ASSINATURA (XML)

Fonte: FIGURA REALIZADA PELO AUTOR

O processo de validação da assinatura digital em XML é dividido em cinco etapas, descritas a seguir:

1. Seleciona-se o arquivo XML assinado;
2. Extrai-se do arquivo XML assinado, os conteúdos das *tag* infNFe para normalização e canonização C14N, das *tags DigestValue*, *SignatureValue*, *X509Certificate*. Os valores coletados são convertidos de *base64* para hexadecimal, para a extração do *hash* esperado, a assinatura e o certificado X509, este último contém a chave pública. Posteriormente remove-se da *tag* NFe, a *tag Signature*, para se gerar um novo arquivo XML. Este procedimento é feito para verificação posterior da assinatura digital e também se o conteúdo da NF-e se está integro ou não;
3. Após a etapa anterior, é gerado um novo *hash* via SHA1 da tag <infNFe> do arquivo XML;
4. Para o processo de validação, se faz necessário enviar para a classe *Signature*, os valores da chave pública do Certificado X509, a assinatura e o novo *hash* gerado arquivo XML, do qual foi removida a tag *signature*;
5. Por fim o método *Verify*(), da classe *Signature*, recebe todos os parâmetros necessário, para efetuar a comparação e apresentar a mensagem validação com sucesso ou não. Com isso é possível garantir não apenas o princípio de autenticidade da assinatura digital do mesmo, e ainda o princípio de integridade dos dados recebidos, de acordo com os conceitos da PSI.

O ambiente de projeto utilizado no desenvolvimento deste protótipo utilizou os seguintes recursos:

- Notebook (core 2 duo 2.0Ghz / 4Gb de ram / SSD 240Gb);
- Leitor de impressão digital da CIS (DigiScan FS 88H edição específica para desenvolvedor), certificado pelos órgãos: FBI segundo a norma PIV-071006, FIPS201 (*Federal Information Processing Standard* 201), PIV (*Personal Identification Verification*) da *Federal Employees and Contractors*, GSA *(General Services Administration*) e FIPS 201 *Evaluation Program*;
- Leitor e gravadora de *smart card* da CIS (SCR 3310 v2.0 RD1-X);
- *Java card* da NXP J2A080 (80k, JCOP 2.4.1, JC 2.2.2, GP 2.1.1, T=1, SCP02);
- Sistema operacional Windows 10 professional 64 Bits;
- Ambiente de desenvolvimento em linguagem *java* (eclipse neo 2.0);

- Plug-in JCDE 0.2;
- JDK 1.8;
- JCDK 2.2.2;
- JC Kit 1.0.5.37;
- JDOM;
- Kit de desenvolvimento SDK do leitor biométrico da CIS;
- Projeto *open source* PKIHostAPI;
- Projeto *open source* PKIApplet;
- XStream 1.4;
- Visualizador de XML (NFe/Cte/NFCe).

5.4 ANÁLISE DOS RESULTADOS

Após a conclusão do projeto e com aplicação nas empresas neste quase experimento, utilizando Autenticação Multifatorial em *Hardware*, em conjunto com o leitor biométrico e o *java card*, em um ambiente simulado, conclui-se que o padrão atual de utilização do PIN numérico para qualquer tipo de *smart card*, *token* ou *etoken* não garante a autenticidade do detentor legítimo do mesmo, conforme demonstra-se nos gráficos das figuras 64, 65, 66 e 67, relacionados aos resultados da pesquisa do tópico 5.1, referente a observação de forma presencial e também através de questionário.

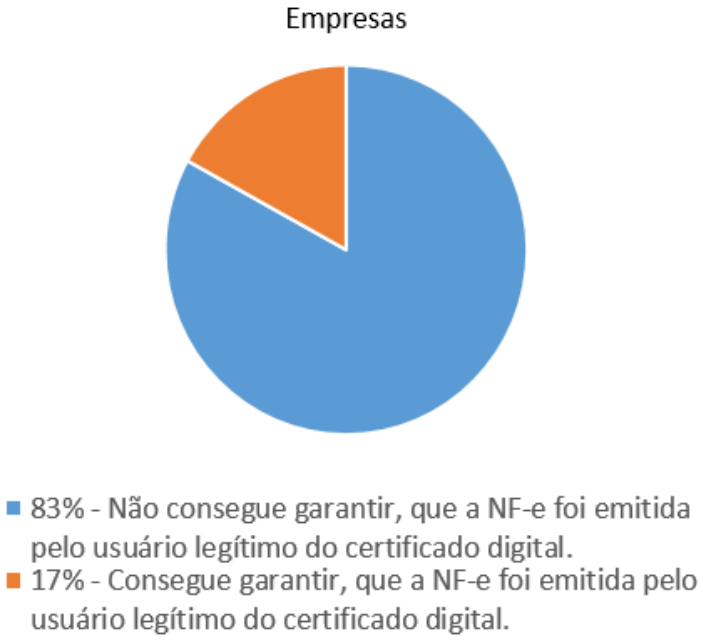


Figura 64 – NF-e EMITIDA PELO USUÁRIO LEGÍTIMO DO CERTIFICADO DIGITAL

Fonte: FIGURA REALIZADA PELO AUTOR

Figura 65 – PROBLEMAS DE EMISSÃO DE NF-e INDEVIDAMENTE

Fonte: FIGURA REALIZADA PELO AUTOR

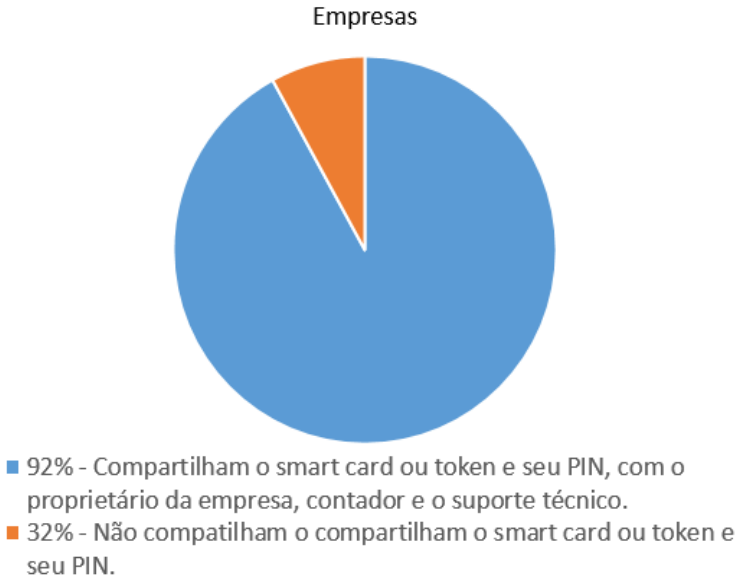


Figura 66 – COMPARTILHAMENTO DE SMART CARD OU TOKEN E SEU PIN

Fonte: FIGURA REALIZADA PELO AUTOR

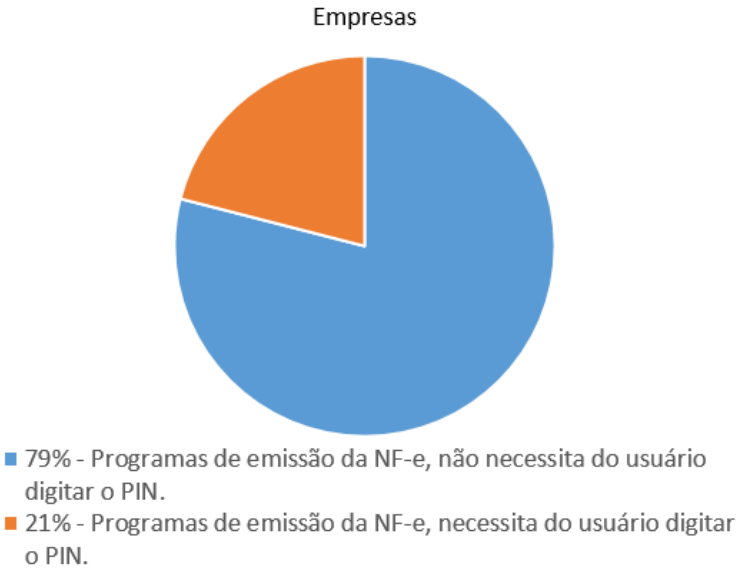


Figura 67 – PROGRAMAS DE EMISSÃO DA NF-e

Fonte: FIGURA REALIZADA PELO AUTOR

Este projeto sugere uma possível solução para este problema, a que foi testada em um grupo composto por 19 mulheres e 11 homens, na faixa de idade entre 25 a 40 anos. Nenhum dos integrantes do grupo conseguiu burlar o sistema de autenticação do PIN biométrico do *java card*, durante os experimentos parcial e final. Durante a fase de testes foi solicitado que os usuários tentassem utilizar técnicas para fraudar o sistema, como por exemplo, o uso de dedo de silicone, entre outros, porém não obteram sucesso.

No processo de avaliação de autenticação do sistema biométrico, foram avaliados também dois aspectos importantes:

- FRR (*False Rejection Rate*) - Significa a taxa de falsa rejeição. Ou seja, taxa em que o usuário legítimo não consegue autenticar-se no sistema biométrico;
- FAR (*False Acceptance Rate*) - Significa a taxa de falsa aceitação, em que o usuário conseguiu burlar o sistema de autenticação biométrico.

Demonstram-se na tabela 14, os resultados do experimento parcial e final, aplicados durante 18 meses nas 20 empresas participantes, quanto ao uso de nossa proposta de solução em um ambiente de assinatura de NF-e simulado, verificando as taxas de FRR e FAR do sistema de autenticação do sistema biométrico.

Tabela 14 – RESULTADOS DO EXPERIMENTO PARCIAL E FINAL

			Resultados			
Usuários	**Tentativas por Usuário**	**Total de Testes**	***False Rejection Rate* (FRR)**	***False Acceptance Rate* (FAR)**	**FRR (%)**	**FAR (%)**
30	30	900	7	0	0,77	0

Fonte: TABELA REALIZA PELO AUTOR

Diante dos fatos apresentados na tabela 14, conseguimos que a FAR ficasse em 0%, demonstrando-se que a proposta aqui apresentada obteve bons resultados para o universo de testes utilizados. Porém, vale ressaltar que alguns dos usuários legítimos do *java card* não conseguiram fazer a autenticação com seus PIN biométricos, devido ao não posicionamento adequado do dedo, durante seu escaneamento ou até mesmo a pressão indevida do dedo no vidro do leitor, deixando-se assim a FRR em 0,77%. O leitor de reconhecimento de impressão digital LFD, possui algoritmos que verificam vários fatores como: pressão do dedo sobre o vidro, rotação do dedo durante a captura e entre outros.

Outro fator importante é que houve um aumento do nível de segurança da aplicação de emissão da NF-e, saindo do nível de segurança 2, padrão técnico do manual de orientação do contribuinte v6.00 (ENCAT, 2015), para o nível de segurança 3 que é proposto nesta solução.

Como pode ser observado no gráfico da figura 68, a proposta sugerida neste projeto comtempla os requisitos do nível de segurança 3.

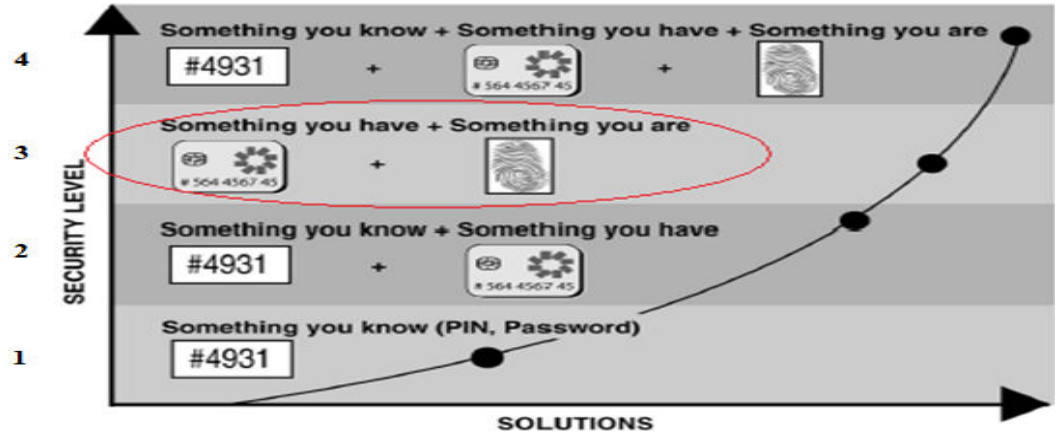


Figura 68 – SOLUTIONS (SECURITY LEVEL)

Fonte: FIGURA REALIZADA PELO AUTOR, ADAPTADA DE OGBANUFE (2017)

Observou-se que durante a pesquisa, tanto com a participação dos funcionários das empresas, como também através da revisão da literatura, não haveria necessidade de se aumentar o nível de segurança da aplicação de emissão da NF-e para nível 4, pois como vimos em capítulos anteriores, senhas podem ser facilmente descobertas ou compartilhadas. Ainda em relação a classificação do nível de segurança para qualquer aplicação, deve-se levar em conta o valor da informação para o usuário, empresa ou órgão público.

Na tabela 15, segue-se um comparativo entre os trabalhos relacionados do tópico 3, que iremos compará-los, com os benefícios propostos pela solução apresentada desta pesquisa.

Tabela 15 – COMPARAÇÃO ENTRE TRABALHOS RELACIONADOS

Trabalhos Relacionais pelos Autores	**Autenticação da Aplicação para *Smart Card***	**Tipos de PIN**	**Presença de Código de Segurança (*Template* Biométrico)**	**Criptografia Dentro ou Fora do *Java Card***	**Nível de Segurança**
BARBOZA (2018)	Sim	Biométrico	Sim	Dentro	Alto
ENCAT (2015)	Não	Numérico	Não	Fora	Baixo
NEDJAH, ET AL., (2017)	Não	Biométrico	Não	Não utiliza	Médio
SILVA (2017)	Não	Numérico	Não	Fora	Baixo
PATIL, ET AL., (2017)	Não	Biométrico	Não	Não utiliza	Médio
PARTOUCHE, ET AL., 2012	Não	Biométrico	Não	Não utiliza	Médio

Fonte: TABELA REALIZA PELO AUTOR

Observe que a proposta sugerida é a única que tem autenticação prévia, isto evita que a aplicação servidor (*applet*) responda para qualquer tipo de aplicação cliente (*host*). Foi utilizado PIN biométrico para evitar compartilhamento do *smart card*. O PIN biométrico possui código de segurança, que a cada sessão é mudada de forma aleatória e criptografada, evitando assim, que se o *template* biométrico seja copiado, e que a aplicação servidor (*applet*) não permita autenticação.

Destaca-se também, que foi possível efetuar toda a parte de criptografia dentro do *smart card*, evitando assim, que a aplicação cliente (*host*) consiga capturar a chave privada e seu respectivo PIN.

Outro fator importante, é que ressaltamos a necessidade de mudar a forma do modelo atual de emissão de certificado tipo A3, de forma pré-personalizada, para a forma personalizada com PIN biométrico sem o PUK, de maneira que apenas nossa proposta proporcionou o cadastramento do usuário, de forma presencial, em um ambiente de simulação da AC.

Diante dos fatos apresentados, observe-se que o modelo proposto de ambiente simulado e seus testes práticos foram plausíveis e satisfatórios, para serem aplicados em um ambiente real, aumentando assim a legitimidade de uma assinatura digital da NF-e.

5.5 BENEFÍCIOS DO SISTEMA PROPOSTO

A proposta para autenticação de NF-e aqui apresentada, pode ser facilmente implantada ao atual sistema, sem grandes ajustes, inserindo as vantagens descritas anteriormente, como descrito a seguir:

- Não é necessário alterar toda a estrutura do processo de emissão da NF-e, adotado pelo ENCAT em conjunto com RFB, para a implantação da metodologia proposta. É preciso apenas modificar a maneira de se assinar digitalmente a NF-e;
- Os procedimentos de comunicação de envio da NF-e, continuam os mesmos por HTTPS e SSL versão 3.0 com autenticação mútua;
- Não é necessário alterar a estrutura de recepção da NF-e do servidor da SEFAZ, ou seja, custo nenhum de implantação desta proposta para a SEFAZ;
- Custo baixo para aplicação desta proposta para a ICP-Brasil e AC's intermediárias, pois só é necessário alterar o PIN (algo que o usuário sabe, ou seja, a senha) no ato

da emissão de um certificado digital, pelo modelo proposto a figura 53, de maneira que a própria amostra biométrica do usuário é a sua senha PIN;

- Custo baixo para aplicação desta proposta, em relação aos benefícios que a mesma propõe para o emitente (empresa), pois só se torna necessário a alteração da maneira de assinar digitalmente a NF-e, pelo programa do emitente (empresa). Neste caso a empresa precisa trocar seu dispositivo de segurança atual (*token* em PC (certificado tipo A1), *token* em *hardware* (certificado tipo A3), e*token* (certificado tipo A3) pelo modelo proposto dos *hardwares* envolvidos na figura 55. Como a maioria das empresas já utilizam uma leitora e um *smart card*, bem como, um PC e uma impressora, só ter-se-ia um custo adicional de aproximadamente R$300,00, para aquisição de um leitor biométrico de reconhecimento de impressão digital com tecnologia LFD;
- O usuário por sua vez, não precisa estar memorizando o PIN do *java card* (certificado tipo A3), pois a própria amostra biométrica do usuário é a sua senha;
- Aumento da segurança da emissão da NF-e, pois é eliminado o uso indevido do *java card* (certificado tipo A3) por pessoas não autorizadas;
- FRR de 0,77% e a FAR de 0%, referente à autenticação com o PIN biométrico, onde demonstra-se a eficácia de se utilizar um leitor biométrico de reconhecimento de impressão digital LFD;
- Aumento da autenticidade da assinatura digital, pois elimina a possibilidade de outro usuário se passar pelo usuário legítimo do certificado digital;
- Aumento do serviço de não-repúdio, em relação à assinatura digital da NF-e.;
- Garante o princípio de integridade dos dados contidos da NF-e;
- Pré-autenticação prévia, para comunicação entre aplicação cliente (*host*) e aplicação servidor (*applet*), com o uso de criptografia simétrica;
- Proteção do *template* biométrico com código de segurança, durante a comunicação e autenticação do sistema, com o uso de criptografia simétrica.

6 CONSIDERAÇÕES FINAIS

Com base no que foi apresentado ao longo desta pesquisa, percebe-se que a proposta da solução apresentada se adequa perfeitamente ao cenário do processo de emissão de NF-e, atualmente vigente em todo Brasil, sugerindo uma solução para o problema de autenticidade e não-repúdio de sua assinatura digital.

Neste contexto foi apresentada uma análise do sistema da NF-e brasileira ora em uso, e proposta uma nova metodologia para a melhoria nos processos de segurança na emissão deste tipo de nota e seu sistema de assinatura digital.

Os resultados desta pesquisa podem beneficiar sobre maneira a SEFAZ, desde que a partir de então ela terá um maior respaldo jurídico, no quesito de autenticidade da NF-e, pois nenhuma empresa poderá alegar desconhecimento (não-repúdio) de tal NF-e.

Para as empresas que emitem NF-e, este projeto beneficia o aumento de segurança no sistema, dificultando assim a emissão de NF-e por pessoas não autorizadas.

No tocante a trabalhos acadêmicos, esta pesquisa pode trazer benefícios, e incentivar o desenvolvimento de projetos de pesquisa aplicadas, em sistemas biométricos e suas aplicações, cada vez mais presentes em sistema de informação.

6.1 LIMITAÇÕES DO TRABALHO

Como limitação do trabalho tem-se as questões referentes à tecnologia do *java card*, pois a mesma não trabalha com ponto flutuante, bem como, o poder computacional de processamento e memória são baixos no *smart card*.

Já em relação a biometria, seria conhecer e implementar novas técnicas da tecnologia LFD no leitor DigiScan FS 88H, pois a empresa CIS só forneceu a CIS_SDK.DLL para ambiente de desenvolvimento, utilizando seus próprios métodos.

Em relação ao tipo de certificado, foi utilizado certificados *.DER, fornecidos pelo projeto *open source* PKI, o qual se faz necessário para utilização em um ambiente real usar certificados válidos, fornecidos por alguma AC autorizada pelo ICP-Brasil, para poder ser validado a assinatura da NF-e pelo site do validador da RF (Receita Federal).

Por fim, para que possamos colocar em ambiente de produção, a nossa proposta teria que obter parceria com a ICP-Brasil e o ENCAT em conjunto com RFB, para que tal tecnologia fosse aceita pelo governo brasileiro.

6.2 TRABALHOS FUTUROS

Para trabalhos futuros, verifica-se a necessidade de implantar um novo modelo de certificado tipo A3, agora sendo personalizado, junto com a certificadora raiz ICP-Brasil, para testar sua eficácia em um ambiente de produção.

Destaca-se a necessidade de levantar um estudo com mais empresas de médio porte e principalmente grande porte, para verificar de forma generalizada, se ocorre o mesmo tipo de problema de segurança da informação, quanto ao compartilhamento e a legitimidade do uso do certificado digital tipo A3, pelo proprietário.

Um outro ponto importante é o estudo e a possível substituição do padrão SHA-1, adotado no manual de orientação do contribuinte (ENCAT, 2015), por outros tipos de algoritmo de resumo (*hash*), como por exemplo o SHA-256 ou superior e testar um mesmo em um ambiente simulado.

Um outro aspecto a ser considerado é a adoção de padrões mais robustos, novas formas de algoritmos criptográficos com chaves de 2048 bits, realidade em outros sistemas, como por exemplo em transações bancárias, devido os avanços tecnológicos do poder computacional em quebrar o algoritmo RSA, através de ataque por força bruta em tempo hábil.

REFERÊNCIAS

ABNT (Associação Brasileira de Normas Técnicas). **ISO/IEC 27002:2013**. Disponível em <http://www.inf.furb.br/~paulofernando/downloads/risco/ISO-27002-2013.pdf>. Acessado em 1 de março de 2017.

ALEJO, Willy; CÁRHUAZ, Daniel Rodríguez; KEMPER, Guillermo. ***Biometric method based on the matching of dilated and skeletonized ir images of the veins map of the dorsum of the hand***. Disponível em <https://ieeexplore.ieee.org/document/7112000/>. Acessado em 17 de outubro de 2015.

ARAÚJO, Paulo Gabriel Ribacionka Góes de. **Sistema de controle de acesso via *smart card* com autenticação biométrica da impressão digital**. Disponível em <http://www.repositorio.uniceub.br/bitstream/123456789/3382/3/20516507.pdf>. Acessado em 1 de dezembro de 2016.

ASSUNÇÃO, Paulo Sergio de S. L. de; MENDONÇA, Luziane F. de. **Detecção e reconhecimento de minúcias em imagens datiloscópicas: uma abordagem holística**. Disponível em <https://proceedings.sbmac.org.br/sbmac/article/viewFile/660/666>. Acessado em 28 de dezembro de 2015.

BARROSO, Bruno Lemos. **Criptografia: aspectos teóricos e proposta de autenticação utilizando dados cadastrais do usuário**. Disponível em <https://pantheon.ufrj.br/bitstream/11422/3328/4/BBarroso.pdf>. Acessado em 29 de maio de 2016.

BLOKDYK, Gerardus. ***Smart card management system: the ultimate step-by-step guide***. Rio de Janeiro: 5STARCooks, 2018.

BOENTI, A.; BRAGA, G. **Metodologia científica contemporânea para universitários e pesquisadores.** Rio de Janeiro: Brasport, 2004.

BONEH, Dan. ***Criptography I***. Disponível em <http://www.coursera.com>. Acessado em 15 de março de 2017.

BORTOLINI, Rafael. **Precisamos falar sobre problemas de certificados digitais no Brasil**. Disponível em <https://proceedings.sbmac.org.br/sbmac/article/viewFile/660/666>. Acessado em 20 de março de 2017.

BRAGANÇA, Karina França; SILVA, Silvana Leal da; SANTOS, Ramon Chagas. **Criptografia: uma ferramenta para o estudo de função afim e de sua inversa**. Disponível em <http://licenciaturas.centro.iff.edu.br/cursoslicenciatura/licenciatura-em-matematica/trabalho-de-conclusao-de-curso/2017/CRIPTOGRAFIA%20UMA%20FERRAMENTA%20PARA%20O%20ESTUDO%20DE%20FUCAO%20AFIM%20E%20SUA%20INVERSA.pdf/at_download/file>. Acessado em 21 de novembro de 2017.

CAMPOS, Jonilson Batista. **Como funcionam os sistemas de biometria: um estudo geral**. Disponível em <http://www.doctum.com.br/unidades/teofilootoni/graduacao/sistemadeinformacao/artigos/art

igo_professor_jonilson.doc>. Artigo presente na Pós-Graduação em Redes e *E-comerce* das Faculdades Integradas de Caratinga (FIC/MG) no ano de 2007. Acessado em 24 de julho de 2011.

CERTISIGN. **Tipos e *drivers* de *token***. Disponível em <https://www.certisign.com.br/duvidas-suporte/downloads/tokens>. Acessado em 5 de julho de 2017.

CASADO, Ricardo Salvino. **Extração de minúcias em imagens de impressões digitais**. Disponível em <http://www.teses.usp.br/teses/disponiveis/18/18152/tde-15102008-135808/pt-br.php>. Dissertação de mestrado presente na USP no ano de 2008. Acessado em 2 de julho de 2016.

CIS. **Manual de sistema de integração biométrica**. Disponível em <https://www.cis.com.br>. Acessado em 24 de fevereiro de 2017.

CIS. **Leitores de código de barras, cheques e cartões**. Disponível em <https://www.cis.com.br/produtos/leitores>. Acessado em 2 janeiro de 2018.

CHEN, Zhiqun. ***Java card technology for smart cards***. 2° Edição. Editora Person Education, 2000.

DEMO, Pedro. **Metodologia do conhecimento científico.** São Paulo: Editora Atlas, 2000.

DEVMEDIA. **Como funciona a criptografia *hash* em java.** Disponível em <https://www.devmedia.com.br/como-funciona-a-criptografia-hash-em-java/31139>. Acessado em 20 de setembro de 2014.

DOLCE, Lucas Plis; SILVA, Francisco Assis da; CARRO, Silvio Antônio. **Utilização de *java card* como plataforma para o desenvolvimento de aplicações em *smart card***. Disponível em <http://revistas.unoeste.br/revistas/ojs/index.php/ce/article/viewFile/720/928>. Acessado em 20 de outubro de 2013.

DUARTE, Felipe Simões Lage Gomes. **Auditoria e segurança de sistemas (criptografia)**. Disponível em <http://www.felipelageduarte.com.br/courses/20150201/Aula08.pdf>. Acessado em 15 de fevereiro de 2016.

ENCAT. **Ato COTEPE 14-2009: manual de emissão da NF-e em contingência**. Disponível em <http://www.fazenda.gov.br/confaz/confaz/Diversos/ATO_COTEPE_14-09_-_MANUAL_DA_CONTINGENCIA.pdf>. Acessado em 24 de julho de 2011.

ENCAT. **Manual de orientação do contribuinte v6.00**. Disponível em <https://www.nfe.fazenda.gov.br/portal/listaConteudo.aspx?tipoConteudo=33ol5hhSYZk=>. Acessado em 15 de dezembro de 2015.

ENCAT. **Projeto nota fiscal eletrônica**. Disponível em <http://www.nfe.fazenda.gov.br/portal/exibirArquivo.aspx?conteudo=%20tq7zNwy6jo=>. Acessado em 10 de agosto de 2016.

FADEL, Désirée Faria. **Teoria aritmética dos números**. Disponível em <https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/desi_RSA.pdf>. Acessado em 28 de setembro de 2009.

FERREIRA, Anderson Luís de Sousa; MOTA, José dos Reis. **Aplicação de reconhecimento biométrico por meio de impressão digital no centro universitário de Patos de Minas**. Disponível em <http://perquirere.unipam.edu.br/documents/23700/1025842/Aplicacao+do+reconhecimento+biometrico.pdf>. Acessado em 18 de dezembro de 2015.

FUTRONIC. **Ficha informativa sobre a tecnologia *Live Finger Detection* (LFD) da Futronic**. Disponível em <http://www.futronic-tech.com/product_lfd.html>. Acessado em 9 de agosto de 2017.

GAMA, Vitor Sad Cortat Xavier da; NASCIMENTO, Franciele Lucas do; CASTRO, Hitalo dos Santos; BENTO, Leonardo Ferreira. **Certificado digital: um estudo sobre os efeitos da implantação do sistema de certificação digital nas empresas de contabilidade da região**. Disponível em <http://pensaracademico.facig.edu.br/index.php/semiariocientifico/search/search?query=CERTIFICADO+DIGITAL%3A+UM+ESTUDO+SOBRE&authors=&title=&abstract=&galleyFullText=&suppFiles=&dateFromMonth=&dateFromDay=&dateFromYear=&dateToMonth=&dateToDay=&dateToYear=&dateToHour=23&dateToMinute=59&dateToSecond=59&discipline=&subject=&type=&coverage=&indexTerms=>. Acessado em 18 de dezembro de 2017.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4º Edição. São Paulo: Editora Atlas, 2008.

GOMES, Bruno Emerson Gurgel. **Desenvolvimento formal de aplicações para *smart cards***. Disponível em <https://repositorio.ufrn.br/jspui/bitstream/123456789/17947/1/BrunoEGG_TESE.pdf>. Acessado em 28 de outubro de 2012.

GUO, Norman. ***Smart card operation using freescale microcontrollers***. Disponível em <https://www.nxp.com/docs/en/application-note/AN4453.pdf>. Acessado em 2 de novembro de 2012.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002**. 1º Edição. Rio de Janeiro: Editora Brasport, 2018.

IBGE. **Pesquisa Anual de Comércio (PAC)**. Disponível em < https://www.ibge.gov.br/estatisticas-novoportal/economicas/comercio/9075-pesquisa-anual-de-comercio.html?=&t=o-que-e>. Acessado em 1 de dezembro de 2016.

ISO. **ISO/IEC 7816-3:2006** ***Identification cards - integrated circuit cards - part 3: cards with contacts - electrical interface and transmission protocols***. Disponível em <https://www.iso.org/standard/38770.html>. Acessado em 6 de agosto de 2016.

ISO. **ISO/IEC 7816-4:2013** ***Identification cards - integrated circuit cards - part 4: organization, security and commands for interchange***. Disponível em <https://www.iso.org/standard/54550.html>. Acessado em 8 de agosto de 2016.

ITI. **ICP-Brasil**. Disponível em <http://www.iti.gov.br/icp-brasil>. Acessado em 28 de abril de 2018.

JAMHOUR, Edgard. **Criptografia: assinaturas digitais e certificados digitais**. Disponível em <https://slideplayer.com.br/slide/345206/>. Acessado em 20 de outubro de 2013.

JANES, Ricardo. **Proposição de um algoritmo para identificação biométrica de pessoas baseado nos padrões de veias das mãos**. Disponível em <http://www.teses.usp.br/teses/disponiveis/3/3143/tde-20072016-082931/pt-br.php>. Acessado em 20 de novembro de 2016.

JONG, Eduard de; PIETER, Hartel; PEYRET, Patrice; CATTANEO, Peter. ***Java card: an analysis of the most successful smart card operating system to date***. University Twente, 2005. Disponível em <https://research.utwente.nl/en/publications/java-card-an-analysis-of-the-most-successful-smart-card-operating>. Acessado em 10 de outubro de 2016.

KATZ, Jonathan; LINDELL, Yehuda. ***Introduction to modern cryptography***. 2ª Edição. Flórida: CRC Press, 2014.

KERBY, Fred. ***Two factor authentication***. Disponível em <http://www.securingthehuman.org>. Acessado em 15 de dezembro de 2012.

KIM, David; SOLOMON, Michael G. **Fundamentos de segurança de sistemas de informação**. 1º Edição. Rio de Janeiro: Editora LTC, 2014.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação gerenciais: administrando a empresa digital**. 5ª Edição. São Paulo: Pearson, 2005.

MACHADO, Robson Carvalho. **Certificação digital:** ICP-Brasil. 1ª Edição. Impetus, 2010.

MARCHIORO, Fernanda. **Nota fiscal eletrônica diminui significativamente a sonegação de impostos**. Disponível em <https://www.notanet.com.br/nota-fiscal-eletronica-diminui-significativamente-a-sonegacao-de-impostos/>. Acessado em 15 de setembro de 2011.

MARGATO, Victor. **Sped: informatização das obrigações levará a supercontrole**. Disponível em <http://www.artigonal.com/financas-pessoais-artigos/sped-informatizacao-das-obrigacoes-levara-a-supercontrole-5190634.html>. Acessado em 13 de setembro de 2011.

MARTINA, Jean Everson; BOAL, Luiz Augusto Chaves. **Uma análise formal automatizada dos protocolos de envio e confirmação de processamento da nota fiscal eletrônica brasileira**. Artigo presente nos anais do VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais de 2008.

MATOS, Conrado Leiras. ***Smart card***. Documento presente no Grupo de Teleinformática e Automação da Universidade Federal do Rio de Janeiro (UFRJ) no ano de 2003. Disponível em <http://www.gta.ufrj.br/grad/01_2/smartcard/smartcard.html>. Acessado em 5 de setembro de 2011.

MELO, Guilherme Nunes. **Sistema de identificação biométrica baseado no código de íris combinado com códigos corretores de erros**. Disponível em <https://repositorio.ufpe.br/bitstream/123456789/23623/1/Tese%20-%20Guilherme%20Nunes%20Melo.pdf>. Acessado em 24 de setembro de 2016.

MOUTA, Albert Eije Barreto. **Manual de implantação da NFC-e *desktop***. 1º Edição. Editora Albert Eijer, 2015.

MOUTA, Albert Eije Barreto. **Manual de implantação da nota fiscal eletrônica**. 2ª Edição. Rio de Janeiro: Ciência Moderna Ltda, 2010.

NASCIMENTO, João Pedro Alves P do; HENRIQUES, Marco Aurélio Amaral. **Avaliação do desempenho e do consumo de memória de uma implementação do algoritmo de chave simétrica Rijndael**. Relatório técnico DCA-RT 01/01, 2001.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes coorporativos.** 1ª Edição. Novatec Editora Ltda, 2007.

NEDJAH, Nadia; WYANT, Rafael Soares; MOURELLE, Luiza de Macedo; GUPTA, Brij Bhushan. ***Efficient fingerprint matching on smart cards for high security and privacy in smart systems***. Disponível em <https://doi.org/10.1016/j.ins.2017.12.038>. Acessado em 30 de setembro de 2017.

NUNES, Fernanda Todesco. **Técnicas de biometria baseadas em padrões faciais e sua utilização na segurança pública**. Disponível em <http://posticsenasp.ufsc.br/files/2015/07/mono_fernanda_rv3_final.pdf>. Acessado em 21 de dezembro de 2015.

OFTALMOS. ***Nuevo tratamiento con láser del glaucoma***. Disponível em <https://clinicaoftalmos.wordpress.com/category/glaucoma/>. Acessado em 11 de dezembro de 2012.

OGBANUFE, Obi; KIMB, Dan J. ***Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment***. Disponível em <https://doi.org/10.1016/j.dss.2017.11.003>. Acessado em 1 de dezembro de 2017.

OLIVEIRA, Déborah. ***Java*** **completa 20 anos: veja trajetória da linguagem de programação**. Disponível em <https://www.itforum365.com.br/tecnologia/java-completa-20-anos-veja-trajetoria-da-linguagem-de-programacao/>. Acessado em 1 de setembro de 2015.

OLIVEIRA, Magda Vieira da Silva; SANTOS, Melina Rossi. **Últimos cinco anos de pesquisa em biometria: um estudo das principais universidades no Brasil**. Disponível em <http://www.forscience.ifmg.edu.br/forscience/index.php/forscience/article/download/108/115>. Acessado em 1 de setembro de 2016.

ORACLE. ***Java card technical documents***. Disponível em <http://www.oracle.com/technetwork/java/embedded/javacard/documentation/javacard-docs-1970421.html>. Acessado em 15 de junho de 2018.

PARTOUCHE, Patrick; BLOT, Philippe; MOBETIE, Didier. ***Multiple application chip card having biometric validation***. Disponível em <https://worldwide.espacenet.com/publicationDetails/description?CC=CN&NR=102834829A&KC=A&FT=D&ND=3&date=20121219&DB=&locale=en_EP>. Acessado em 12 de dezembro de 2012.

PATIL, Sonali; DHUMAL, Priyanka; LOKHANDE, Shweta; KAMBLE, Trishala. ***Design and implementation of secure biometric based authentication system using RFID and secret sharing***. Disponível em <https://ieeexplore.ieee.org/document/8226175>. Acessado em 7 de agosto de 2017.

PAULINO, Caroline Rizzi. **SPED fiscal: novas legislações e a tecnologia**. Disponível em <https://www.mega.com.br/blog/sped-fiscal-novas-legislacoes-e-a-tecnologia-9331>. Acessado em 15 de dezembro de 2016.

PEREIRA, Fabio Ciolari. **Desmaterialização de contratos físicos na concessão de crédito consignado em uma instituição financeira**. Disponível em <http://paineira.usp.br/lassu/wp-content/uploads/2016/09/Monografia-Fabio-Ciolari-Pereira.pdf>. Acessado em 25 de outubro de 2016.

PEREIRA, Samaris Ramiro. **Certificação digital através do algoritmo RSA**. Disponível em <http://www.fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/9>. Acessado em 15 de novembro de 2016.

PINHEIRO, José Maurício. **Biometria nos sistemas computacionais:** você é a senha. 1ª Edição. Editora Ciência Moderna Ltda, 2008.

PORTAL DA NF-e. **Sobre a NF-e**. Disponível em <http://www.nfe.fazenda.gov.br/portal/sobreNFe.aspx?tipoConteudo=HaV+iXy7HdM=#mQhuA1Z2dCo=>. Acessado em 11 de fevereiro de 2017.

PORTAL DA NF-e. **Manual de integração: contribuinte versão 6.00**. Disponível em <http://www.nfe.fazenda.gov.br/Portal/listaConteudo.aspx?tipoConteudo=33ol5hhSYZk=>. Acessado em 28 de dezembro de 2015.

PORTAL ENAT. **Histórico**. Disponível em <http://www19.receita.fazenda.gov.br/enat/historico>. Acessado em 15 de novembro de 2016.

PRESIDÊNCIA DA REPÚBLICA. **Medida provisória nº 2.200-2, de 24 de agosto de 2001**. Disponível em <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acessado em 14 de agosto de 2017.

PRESIDÊNCIA DA REPÚBLICA DA CASA CIVIL. **Emenda constitucional nº 42, de 19 de dezembro de 2003**. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc42.htm>. Acessado em 10 de agosto de 2016.

PROJREDES. **Cifra de bloco**. Disponível em <http://www.projetoderedes.com.br/artigos/artigo_cifras_em_bloco_cifras_de_fluxo.php>. Acessado em 10 de outubro de 2015.

RECEITA FEDERAL DO BRASIL. **Carga tributário no Brasil 2016: análise por tributos e bases de incidência**. Disponível em <http://idg.receita.fazenda.gov.br/dados/receitadata/estudos-e-tributarios-e-aduaneiros/estudos-e-estatisticas/carga-tributaria-no-brasil/carga-tributaria-no-brasil-capa>. Acessado em 11 de dezembro de 2016.

REIS OFFICE. **NF-e: logística da informação**. Disponível em <http://www.reisoffice.com.br/servico/nf-e.asp>. Acessado em 31 de julho de 2011.

REVISTABW. **Segurança de computadores e da informação: métodos de autenticação de usuário**. Disponível em <https://www.revistabw.com.br/revistabw/seguranca-autenticacao-de-usuario/>. Acessado em 28 de setembro de 2016.

REVISTAGETHOME. ***Type of smart card***. Disponível em <http://revistagethome.com/bullnet-system.html#>. Acessado em 2 de julho de 2017.

RIBEIRO, Alexandre Menezes; OLIVEIRA, Evandro Luiz de; CARDOSO, Pedro Pinheiro; BERTOL, Viviane Regina Lemos. **A infra-estrutura de chaves públicas brasileira e suas bases para a auditoria em segurança da informação**. Instituto Nacional de Tecnologia (ITI), Brasília, novembro de 2004. Disponível em <http://www.modulo.com.br/pdf/artigo_iti.pdf>. Acessado em 1 de julho de 2005.

RIBEIRO, Raphael Soares. ***Smart card* com tecnologia *java card***. Programa de pós-graduação em engenharia eletrônica da UERJ. Disponível em <http://www.ebah.com.br/content/ABAAABIXIAJ/java-card-basico>. Acessado em 1 de julho de 2015.

RICARDO, Diógenes; CÉSAR, Luan. **Uma proposta de identificação de impressões digitais empregando redes neurais artificiais**. Disponível em <https://pt.slideshare.net/diogenesrfreitas/proposta-de-identificao-de-impresses-digitais-empregando-redes-neurais-artificiais>. Acessado em 10 de dezembro de 2012.

ROSA JUNIOR, Laerte Clademir da. **Proposta de certificação digital para medidores inteligentes de energia elétrica**. Programa de pós-graduação em Desenvolvimento de Tecnologia do Instituto de Tecnologia para o Desenvolvimento, em parceria com o Instituto de Engenharia do Paraná. Disponível em <http://www.lactec.org.br/wp-content/uploads/download.php?arquivo=2017/07/dissertacao_Laerte_final_corrigida-VF.pdf>. Acessado em 5 de dezembro de 2015.

RUGGIERO, Wilson Vicente; VIEIRA, Gustavo Yamasaki Martins. **Algoritmos para *tokens* de autenticação.** Artigo presente nos anais da conferência IADIS Ibero-Americana WWW/Internet2007 no ano de 2007. Disponível em <http://www.iadis.net/dl/final_uploads/200713L020.pdf>. Acessado em 5 de novembro de 2011.

SAFENET. ***eToken* NG-FLASH da Aladim estreia-se como a primeira unidade de autenticação que incorpora flash encriptado e a tecnologia flexível de *java card***. Lisboa, 9 de abril de 2008. Disponível em <http://www3.safenet-inc.com/news/2008/eToken/ng-flash-java-combo-pt.aspx>. Acessado em 11 de novembro de 2017.

SAFEWEB. **Comprar certificado digital: passo a passo**. Disponível em <https://blog.contadorparceirosafeweb.com.br/comprar-certificado-digital-passo-a-passo-e9caca8ce161>. Acessado em 21 de dezembro de 2015.

SANTOS, Danilo de Carvalho. **A nota fiscal eletrônica – NF-e: como ferramenta contra a evasão fiscal**. Disponível em <http://www.artigos.netsaber.com.br>. Acessado em 25 dezembro de 2012.

SEBRAE. **Anuário do trabalho nos pequenos negócios**. Disponível em <https://m.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/Anuario%20do%20Trabalho%20nos%20Pequenos%20Neg%C3%B3cios%202016_.pdf>. Acessado em 1 dezembro de 2016.

SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO. **Nota fiscal eletrônica**. Disponível em <https://www.fazenda.sp.gov.br/nfe/historico/historico.asp>. Acessado em 12 de setembro de 2016.

SETESYS. **Cifra de César**. Disponível em <https://www.setesys.com.br/blog/como-produzir-senhas-criativas-utilizando-a-cifra-de-cesar>. Acessado em 12 de dezembro de 2016.

SILVA, Igor Martins. C**riptografia no processo judicial eletrônico e na análise de provas digitais**. Disponível em <http://www.bdm.unb.br/handle/10483/17848>. Acessado em 14 de setembro de 2017.

SILVA, Luiz Gustavo Cordeiro da; SILVA, Paulo Caetano da; BATISTA, Eduardo Mazza; HOMOLKA, Herbert Otto; AQUINO, Ivanildo José De Sousa, LIMA, Marcelo Ferreira de. **Certificação digital: conceitos e aplicações (modelos brasileiro e australiano)**. 1ª Edição. Rio de Janeiro: Ciência Moderna Ltda, 2008.

SINGH, Simon. **O livro dos códigos**. 1º Edição. São Paulo: Editora Record, 2007.

SOUSA, Jucélio Praciano Rodrigues. **Impactos da utilização da nota fiscal eletrônica nas atividades de monitoramento e fiscalização do ICMS: um estudo na secretária da fazenda do estado do Ceará**. Dissertação presente na Pós-Graduação em Administração e Controladoria da UFCE/CE, em 2010. Disponível em <http://www.repositorio.ufc.br/handle/riufc/15592>. Acessado em 12 de janeiro de 2016

SOUSEDIK, Ctirad; BUSCH, Christoph. ***Presentation attack detection methods for fingerprint recognition systems***. Disponível em <https://ieeexplore.ieee.org/ielx7/6072579/6985790/06985813.pdf?tp=&arnumber=6985813&isnumber=6985790>. Acessado em 12 de dezembro de 2013.

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de sistemas de informações.** 4º Edição. Editora LTC, 2002.

STEVENSON, Angus; WAITE, Maurice. ***Concise oxford english dictionary***. 12° Edição. USA: Oxford University Press Edition, 2016.

SUPREMA. ***Suprema's live dinger detection technology***. Disponível em <http://kb.supremainc.com/knowledge/doku.php?id=en:tc_whitepaper_suprema_live_finger_detection>. Acessado em 2 de dezembro de 2016.

SYSTONIC TECNOLOGIA. **Visualizador de XML (NFE/CTE/NFCE)**. Disponível em <www.systronic.com.br>. Acessado em 23 de setembro de 2017.

TECMUNDO. **Como funcionam os sistemas de reconhecimento facial**. Disponível em <https://www.tecmundo.com.br/camera-digital/10347-como-funcionam-os-sistemas-de-reconhecimento-facial.htm>. Acessado em 1 de outubro de 2011.

TECNOSPEED. **Dossiê NFC-e/2013**. Disponível em <www.tecnospeed.com.br>. Acessado em 1 de maio de 2017.

TKOTZ, Viktoria. **Criptografia – segredos embalados para viagem**. São Paulo: Editora Novatec, 2005.

THING, Lowell. **Dicionário de tecnologia**. São Paulo: Editora Futura, 2003.

UFRJ (Universidade Federal do Rio de Janeiro). **Criptografia quântica**. Disponível em <http://www.gta.ufrj.br/grad/10_1/quantica/introducao.html>. Acessado em 1 de março de 2015.

VALCARENGHI, Emily Vivian. **Impactos da adoção da certificação digital ICP-Brasil**. Disponível em <https://repositorio.ufsc.br/bitstream/handle/123456789/159026/337368.pdf?sequence=1&isAllowed=y>. Acessado em 1 de dezembro de 2015.

VIEIRA, Gustavo Yamasaki Martins. **Projeto de um dispositivo de autenticação e assinatura.** Disponível em <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-14012008-162619/publico/GYMVDissertacao.pdf>. Acessado em 6 de novembro de 2016.

WAZLAWICK, Raul Sidnei. **Metodologia de pesquisa para ciência da computação**. 2º Edição. Rio de Janeiro: Editora Elsevier, 2014.

ZANINI, Michel. **Autenticação e assinatura de documentos na internet com política de certificados digitais A3**. Dissertação presente nos anais da Universidade Federal de Santa Catarina no Centro Tecnológico do ano de 2007. Disponível em <http://projetos.inf.ufsc.br/arquivos_projetos/projeto_698/relatorio-projeto1.pdf>. Acessado em 1 de novembro de 2011.

ZOCHIO, Marcelo Ferreira. **Introdução à criptografia**. 1º Edição. São Paulo: Editora Novatec, 2016.

ZUNINO, José Diego. **Certificação digital: assinatura digital, certificados digitais e sua utilização no mercado nacional.** Disponível em <https://publicacao.uniasselvi.com.br/index.php/TI_EaD/article/view/1691>. Acessado em 16 de novembro de 2017.

APÊNDICE A – CARTA DE APRESENTAÇÃO

Prezados PROPRIETÁRIOS E FUNCIONÁRIOS,

Esta é uma pesquisa de Pós-Graduação Stricto Sensu da UFPE (Universidade Federal de Pernambuco) campus universitário de Recife, curso de mestrado acadêmico em Ciência da Computação, a fim de demonstrar a percepção de falhas no processo da assinatura digital da Nota Fiscal Eletrônica (NF-e), o qual se utiliza atualmente com dispositivo de segurança *token* ou *smart card*, nas empresas que ficam próximas do centro comercial da cidade de Caruaru-PE.

A sua participação é fundamental para o avanço desta pesquisa, auxiliando a universidade a tornar o ensino do acadêmico mais adequado ao mercado de trabalho. **Vale lembrar que fica opcional, se quiser ou não se identificar, por motivo pessoal.**

Saiba que você tem o direito de não responder a alguma pergunta, por qualquer que seja o motivo. Lembramos que não existem respostas certas ou erradas, o que importa é sua opinião sincera. Caso não responda ou não opine, peço que sinalize a alternativa correspondente para que possa ter certeza de que não se esqueceu de responder a alguma pergunta.

Lembramos que nenhum dado será divulgado, individualmente ou em grupo, para a empresa em que trabalha, nem tão pouco será mencionado na pesquisa cientifica os nomes dos participantes e em suas respectivas empresas, em que trabalham. Todas as informações serão tabuladas e agrupadas para análise, somente a fins acadêmicos.

Muito obrigado, pela sua participação.

Eudes da Silva Barboza	**Prof. Dr. Manoel Eusébio de Lima**
Mestrando da UFPE	Coordenador da pesquisa
Aluno do CIn/UFPE Campus Recife	Professor do CIn/UFPE Campus Recife

APÊNDICE B – QUESTIONÁRIO

Nome do Participante (Opcional): _____

1. Qual o principal motivo da implantação da nota fiscal eletrônica (NF-e), para empresa?
( ) Obrigatoriedade.
( ) Voluntariedade.
( ) Sistematização dos dados.
( ) Diminuição de gastos.
( ) Outros.

2. Classifique de 1 a 5, sobre os impactos com a implantação da NF-e.
Sendo: 1- Sem Importância (SI); 2- Pouca Importância (PI) 3- Neutro (N); 4- Muita Importância (MI) e 5- Extrema Importância (EI).
( ) Consumo de papel será reduzido com impacto positivo ao meio Ambiente.
( ) Oportunidade de empregos na área de tecnologia em informática.
( ) Facilitou a fiscalização, aumentando a arrecadação de impostos e diminuindo a sonegação.
( ) Diminuiu os custos com equipamentos emissor de Cupom Fiscal.
( ) Não houve benefícios.

3. Classifique de 1 a 5, sobre em quais pontos a NF-e gerou ou poderá gerar benefícios para sua empresa na prestação de serviços contábeis?
Sendo: 1- Sem Importância (SI); 2- Pouca Importância (PI) 3- Neutro (N); 4- Muita Importância (MI) e 5- Extrema Importância (EI).
( ) Redução de custos e consumo de papel.
( ) Eliminação de arquivos.
( ) Redução de erros de escrituração contábil.
( ) Redução de tempo na escrituração contábil.
( ) Aumento na lucratividade do escritório.

4. Dentro da empresa, existe alguma política de segurança da informação (PSI), baseada na ISO 27002:2013?
( ) Sim.
( ) Não.

5. Dentro das normas da empresa, permite o compartilhamento de senhas, dentro ou fora do ambiente de trabalho, entre funcionários?
( ) Sim.
( ) Não.

6. Você tem necessidade de compartilhar senhas, com outros funcionários, para poder executar determinada tarefa?
( ) Sim.
( ) Não.

7. Com o consentimento do proprietário da empresa, você compartilha a senha com algum funcionário, para poder executar determinada tarefa de forma:
( ) Cotidiana.
( ) De vez em quando.
( ) Nunca acontece.

8. Referente as senhas de qualquer sistema de autenticação, dentro da empresa, como por exemplo *login* e senha, é comum utilizar senha padrão, como por exemplo "1234"?
( ) Sim.
( ) Não.

9. Se dentro da empresa existe vários sistemas de autenticação, é comum utilizar a mesma senha para todos?
( ) Sim.
( ) Não.

10. Para facilitar, as tarefas cotidianas do processo de emissão de NF-e, é comum deixar a senha padrão de fábrica (PIN) do *token* ou *smart card* e não a modificar?
( ) Sim.
( ) Não.

11. Para facilitar, as tarefas cotidianas do processo de emissão de NF-e, é comum deixar o seu certificado digital tipo A3, dentro da leitora *smart card*, ou o *token* no PC por um breve período de tempo, como por exemplo: ir ao banheiro, tomar um café, entre outros?
( ) Sim.
( ) Não.

12. Para facilitar as tarefas cotidianas do processo de emissão de NF-e, é comum deixar o seu certificado digital tipo A3, dentro da leitora *smart card*, ou o *token* no PC por um longo período de tempo, como por exemplo: ir almoçar ou mesmo depois do final do expediente?
( ) Sim.
( ) Não.

13. Quantas pessoas na empresa utilizam o mesmo *token* ou *smart card* (certificado digital tipo A3) em conjunto com sua respectiva senha (PIN), para assinar e emitir a NF-e, com o consentimento do real proprietário do *token* ou *smart card*?
( ) 1 pessoa.
( ) 2 pessoas.
( ) 3 pessoas.
( ) 4 pessoas.
( ) Ou mais.

14. Você tem conhecimento de problemas que poderiam ser causados, se alguém não autorizado pelo proprietário da empresa, assinasse e emitisse uma NF-e, utilizando o *token ou smart card* em conjunto com sua respectiva senha (PIN)?
( ) Sim.
( ) Não.

APÊNDICE C – ARQUIVO XML NÃO ASSINADO

```
<?xml version="1.0" encoding="utf-8"?>
<NFe xmlns="http://www.portalfiscal.inf.br/nfe">
   <infNFe Id="NFe43120103987283000133550010000006241607910981" versao="4.00">
     <ide>
       <cUF>43</cUF>
       <cNF>60791098</cNF>
       <natOp>5.101 - VENDA</natOp>
       <indPag>1</indPag>
       <mod>55</mod>
       <serie>1</serie>
       <nNF>624</nNF>
       <dhEmi>2012-01-25</dhEmi>
       <tpNF>1</tpNF>
       <cMunFG>4313409</cMunFG>
       <tpImp>1</tpImp>
       <tpEmis>1</tpEmis>
       <cDV>1</cDV>
       <tpAmb>2</tpAmb>
       <finNFe>1</finNFe>
       <procEmi>0</procEmi>
       <verProc>2.02</verProc>
     </ide>
     <emit>
       <CNPJ>03987283000133</CNPJ>
       <xNome>MINHA EMPRESA TESTE LTDA.</xNome>
       <xFant>MINHA EMPRESA FANTASIA TESTE</xFant>
       <enderEmit>
         <xLgr>RUA TESTE</xLgr>
         <nro>123</nro>
         <xBairro>CENTRO</xBairro>
         <cMun>4312345</cMun>
         <xMun>PORTO ALEGRE</xMun>
         <UF>RS</UF>
         <CEP>93000000</CEP>
         <cPais>1058</cPais>
         <xPais>BRASIL</xPais>
         <fone>5111223344</fone>
       </enderEmit>
       <IE>0868689965</IE>
       <CRT>1</CRT>
     </emit>
     <dest>
       <CNPJ>99999999000191</CNPJ>
       <xNome>NF-E EMITIDA EM AMBIENTE DE HOMOLOGACAO - SEM VALOR
FISCAL</xNome>
       <enderDest>
         <xLgr>AV. DOS TESTES</xLgr>
         <nro>202</nro>
         <xBairro>CENTRO</xBairro>
         <cMun>4369854</cMun>
         <xMun>PORTO ALEGRE</xMun>
```

```
    <UF>RS</UF>
    <CEP>93000000</CEP>
    <cPais>1058</cPais>
    <xPais>BRASIL</xPais>
   </enderDest>
   <indIEDest>ISENTO</indIEDest>
  </dest>
  <det nItem="1">
   <prod>
    <cProd>B17025056</cProd>
    <cEAN></cEAN>
    <xProd>PAPEL MAXPLOT- 170MX250MX56GRS 3&amp;quot;</xProd>
    <NCM>48025599</NCM>
    <CFOP>5101</CFOP>
    <uCom>Rl</uCom>
    <qCom>1.0000</qCom>
    <vUnCom>138.3000</vUnCom>
    <vProd>138.30</vProd>
    <cEANTrib></cEANTrib>
    <uTrib>RL</uTrib>
    <qTrib>1.0000</qTrib>
    <vUnTrib>138.3000</vUnTrib>
    <indTot>1</indTot>
   </prod>
   <imposto>
    <vTotTrib>41.49</vTotTrib>
    <ICMS>
     <ICMSSN101>
      <orig>0</orig>
      <CSOSN>101</CSOSN>
      <pCredSN>2.56</pCredSN>
      <vCredICMSSN>3.54</vCredICMSSN>
     </ICMSSN101>
    </ICMS>
    <IPI>
     <clEnq>48025</clEnq>
     <CNPJProd>00822602000124</CNPJProd>
     <cEnq>599</cEnq>
     <IPINT>
      <CST>53</CST>
     </IPINT>
    </IPI>
    <PIS>
     <PISNT>
      <CST>07</CST>
     </PISNT>
    </PIS>
    <COFINS>
     <COFINSNT>
      <CST>07</CST>
     </COFINSNT>
    </COFINS>
   </imposto>
  </det>
  <det nItem="2">
```

```
  <prod>
    <cProd>1070100752</cProd>
    <cEAN></cEAN>
    <xProd>PAPEL MAXPLOT- 1070X100MX75GRS 2&amp;quot;</xProd>
    <NCM>48025599</NCM>
    <CFOP>5101</CFOP>
    <uCom>RL</uCom>
    <qCom>1.0000</qCom>
    <vUnCom>48.9100</vUnCom>
    <vProd>48.91</vProd>
    <cEANTrib></cEANTrib>
    <uTrib>RL</uTrib>
    <qTrib>1.0000</qTrib>
    <vUnTrib>48.9100</vUnTrib>
    <indTot>1</indTot>
  </prod>
  <imposto>
    <vTotTrib>14.67</vTotTrib>
    <ICMS>
      <ICMSSN101>
        <orig>0</orig>
        <CSOSN>101</CSOSN>
        <pCredSN>2.56</pCredSN>
        <vCredICMSSN>1.25</vCredICMSSN>
      </ICMSSN101>
    </ICMS>
    <IPI>
      <clEnq>48025</clEnq>
      <CNPJProd>00822602000124</CNPJProd>
      <cEnq>599</cEnq>
      <IPINT>
        <CST>53</CST>
      </IPINT>
    </IPI>
    <PIS>
      <PISNT>
        <CST>07</CST>
      </PISNT>
    </PIS>
    <COFINS>
      <COFINSNT>
        <CST>07</CST>
      </COFINSNT>
    </COFINS>
  </imposto>
</det>
<det nItem="3">
  <prod>
    <cProd>B17025056</cProd>
    <cEAN></cEAN>
    <xProd>PAPEL MAXPLOT- 170MX250MX56GRS 3&amp;quot;</xProd>
    <NCM>48025599</NCM>
    <CFOP>5101</CFOP>
    <uCom>Rl</uCom>
    <qCom>1.0000</qCom>
```

```
    <vUnCom>138.3000</vUnCom>
    <vProd>138.30</vProd>
    <cEANTrib></cEANTrib>
    <uTrib>RL</uTrib>
    <qTrib>1.0000</qTrib>
    <vUnTrib>138.3000</vUnTrib>
    <indTot>1</indTot>
   </prod>
   <imposto>
    <vTotTrib>41.49</vTotTrib>
    <ICMS>
     <ICMSSN101>
      <orig>0</orig>
      <CSOSN>101</CSOSN>
      <pCredSN>2.56</pCredSN>
      <vCredICMSSN>3.54</vCredICMSSN>
     </ICMSSN101>
    </ICMS>
    <IPI>
     <clEnq>48025</clEnq>
     <CNPJProd>00822602000124</CNPJProd>
     <cEnq>599</cEnq>
     <IPINT>
      <CST>53</CST>
     </IPINT>
    </IPI>
    <PIS>
     <PISNT>
      <CST>07</CST>
     </PISNT>
    </PIS>
    <COFINS>
     <COFINSNT>
      <CST>07</CST>
     </COFINSNT>
    </COFINS>
   </imposto>
  </det>
  <det nItem="4">
   <prod>
    <cProd>B17040056</cProd>
    <cEAN></cEAN>
    <xProd>PAPEL MAXPLOT - 1.700X400MX 56 GRS 3&amp;quot;</xProd>
    <NCM>48025599</NCM>
    <CFOP>5101</CFOP>
    <uCom>Rl</uCom>
    <qCom>1.0000</qCom>
    <vUnCom>214.5700</vUnCom>
    <vProd>214.57</vProd>
    <cEANTrib></cEANTrib>
    <uTrib>Rl</uTrib>
    <qTrib>1.0000</qTrib>
    <vUnTrib>214.5700</vUnTrib>
    <indTot>1</indTot>
   </prod>
```

```
  <imposto>
   <vTotTrib>64.37</vTotTrib>
   <ICMS>
    <ICMSSN101>
     <orig>0</orig>
     <CSOSN>101</CSOSN>
     <pCredSN>2.56</pCredSN>
     <vCredICMSSN>5.49</vCredICMSSN>
    </ICMSSN101>
   </ICMS>
   <IPI>
    <clEnq>48025</clEnq>
    <CNPJProd>00822602000124</CNPJProd>
    <cEnq>599</cEnq>
    <IPINT>
     <CST>53</CST>
    </IPINT>
   </IPI>
   <PIS>
    <PISNT>
     <CST>07</CST>
    </PISNT>
   </PIS>
   <COFINS>
    <COFINSNT>
     <CST>07</CST>
    </COFINSNT>
   </COFINS>
  </imposto>
 </det>
 <det nItem="5">
  <prod>
   <cProd>B18525056</cProd>
   <cEAN></cEAN>
   <xProd>PAPEL MAXPLOT-1.85MX250MX56GRS 3&amp;quot;</xProd>
   <NCM>48025599</NCM>
   <CFOP>5101</CFOP>
   <uCom>Rl</uCom>
   <qCom>1.0000</qCom>
   <vUnCom>149.8300</vUnCom>
   <vProd>149.83</vProd>
   <cEANTrib></cEANTrib>
   <uTrib>RL</uTrib>
   <qTrib>1.0000</qTrib>
   <vUnTrib>149.8300</vUnTrib>
   <indTot>1</indTot>
  </prod>
  <imposto>
   <vTotTrib>44.95</vTotTrib>
   <ICMS>
    <ICMSSN101>
     <orig>0</orig>
     <CSOSN>101</CSOSN>
     <pCredSN>2.56</pCredSN>
     <vCredICMSSN>3.84</vCredICMSSN>
```

```
      </ICMSSN101>
    </ICMS>
    <IPI>
      <clEnq>48025</clEnq>
      <CNPJProd>00822602000124</CNPJProd>
      <cEnq>599</cEnq>
      <IPINT>
        <CST>53</CST>
      </IPINT>
    </IPI>
    <PIS>
      <PISNT>
        <CST>07</CST>
      </PISNT>
    </PIS>
    <COFINS>
      <COFINSNT>
        <CST>07</CST>
      </COFINSNT>
    </COFINS>
  </imposto>
</det>
<total>
  <ICMSTot>
    <vBC>0.00</vBC>
    <vICMS>0.00</vICMS>
    <vICMSDeson>0.00</vICMSDeson>
    <vBCST>0.00</vBCST>
    <vST>0.00</vST>
    <vProd>689.91</vProd>
    <vFrete>0.00</vFrete>
    <vSeg>0.00</vSeg>
    <vDesc>0.00</vDesc>
    <vII>0.00</vII>
    <vIPI>0.00</vIPI>
    <vPIS>0.00</vPIS>
    <vCOFINS>0.00</vCOFINS>
    <vOutro>0.00</vOutro>
    <vNF>689.91</vNF>
    <vTotTrib>206.97</vTotTrib>
  </ICMSTot>
</total>
<transp>
  <modFrete>1</modFrete>
  <transporta>
    <xNome>Cliente Retira</xNome>
    <xEnder>Rua ,</xEnder>
    <xMun>Sao Paulo</xMun>
    <UF>SP</UF>
  </transporta>
  <vol>
    <qVol>1</qVol>
    <marca>S/m</marca>
    <nVol>S/n</nVol>
    <pesoL>0.0</pesoL>
```

```
        <pesoB>0.0</pesoB>
       </vol>
      </transp>
      <cobr>
       <fat>
        <nFat>992346</nFat>
        <vOrig>689.91</vOrig>
        <vLiq>689.91</vLiq>
       </fat>
       <dup>
        <nDup>992346</nDup>
        <dVenc>2015-04-24</dVenc>
        <vDup>689.91</vDup>
       </dup>
      </cobr>
      <infAdic>
       <infCpl>&amp;quot;DOCUMENTO EMITIDO POR EMPRESA OPTANTE PELO SIMPLES
NACIONAL;NAO GERA DIREITO A CREDITO FISCAL DE IPI&amp;quot;;&amp;quot;PERMITE O
APROVEITAMENTO DE CREDITO DE ICMS NO VALOR DE: R$17,66 CORRESPONDENTE A
ALIQUOTA DE 2.56%&amp;quot;;Vendedor:1 - Guilherme Kavedikado;Valor Aproximado dos Tributos
: R$ 206,97. Fonte IBPT (Instituto Brasileiro de Planejamento Tributario)</infCpl>
      </infAdic>
    </infNFe>
</NFe>
```

ANEXO A – CÓDIGO FONTE - RSA

```
def fatorar ():
    resto = m
    if( m <= 0 ):
       print "Numero invalido!"
    else:
       divisor = 2
       fatores = {}
       soma_divisores = 1
       #fatorar o numero
       while resto >= 0 and divisor <= resto:
           if( resto % divisor == 0 ):
               #salvar o numero de vezes que cada fator aparece (expoentes)
               if( fatores.has_key(divisor) ):
                   fatores[divisor] += 1
               else:
                   fatores[divisor] = 1
                resto = resto // divisor
           else:
               divisor += 1
   print fatores
def euclides():
   a=e
   b=m
   dividendo = a
   divisor = b
   restos = []
   while dividendo%divisor > 0:
       c=dividendo%divisor
```

```
        restos+=[c]
        dividendo=divisor
        divisor = c
    #print "MDC = ", divisor
    #print "Restos da divisao = ", restos
def euclides_estendido():
    resposta = {}
    x = {}
    y = {}
    x[0] = 1
    x[1] = 0
    y[0] = 0
    y[1] = 1
    a1 = e
    a2 = m
    while a1%a2 <> 0:
                quociente1 = a1/a2
                temp1 = a1
                a1 = a2
                a2 = temp1%a2
                x1 = x[0]-(x[1]*quociente1)
                y1 = y[0]-(y[1]*quociente1)
                x[0] = x[1]
                x[1] = x1
                y[0] = y[1]
                y[1] = y1
    resposta[0] = x[1]
    resposta[1] = y[1]
    resposta[2] = a2
    #print "Valor do inverso modular: ", resposta[0]
    print "Sua chave privada sera composta por:"
    print "n = ", n
    print "d = ", resposta[0]
    if resposta[0] < 0:
       print "Chave com valor negativo; tente outra combinacao"
p=input("Digite um numero primo maior ou igual a 17: ")
```

```
q=input("Digite outro numero primo menor que o anterior: ")
n=p*q
m=(p-1)*(q-1)
fatorar()
e = input("Digite um numero primo diferente daqueles que estao antes dos
dois pontos: ")
print "Sua chave publica sera composta por:"
print "n = ", n
print "e = ", e
euclides()
euclides_estendido()
```

Este outro programa, também em Python, realiza a prova de conceito:

```
import math
def cifra():
   a = raw_input("Digite uma mensagem de 3 digitos: ")
   b=" ".join(str(ord(c)) for c in a) # aqui se converte caractere em ASCII
   c=[] #criando uma lista
   c += b.split() #dividindo a lista em pedaços
   print "Voce transmitira a mensagem: ", a
   print "Mensagem em ASCII: ", c
   m1a = input("Digite o valor de e: ")
   m1b = input("Digite o valor de n: ")
   m1=input("Digite o primeiro valor ASCII da mensagem: ")
   mc1 = m1**m1a%m1b
   m2=input("Digite o segundo valor ASCII da mensagem: ")
   mc2 = m2**m1a%m1b
   m3=input("Digite o terceiro valor ASCII da mensagem: ")
   mc3 =m3**m1a%m1b
   print "Mensagem a ser transmitida = ", mc1, mc2, mc3
def decifra():
   m11a =input("Digite o valor de d: ")
   m11b = input("Digite o valor de n: ")
   m11=input("Digite o primeiro valor ASCII da mensagem: ")
   mc11 = m11**m11a%m11b
   m22=input("Digite o segundo valor ASCII da mensagem: ")
   mc22 = m22**m11a%m11b
```

```
    m33=input("Digite o terceiro valor ASCII da mensagem: ")
    mc33 =m33**m11a%m11b
    w = [mc11, mc22, mc33]
    s =  "".join([chr(r) for r in w])
    print "Mensagem recebida em texto puro: ", s
    print "Mensagem recebida em ASCII: ", mc11, mc22, mc33
x = input("Escolha a opcao 1 para cifrar ou 2 para decifrar: ")
if x == 1:
   cifra()
elif x == 2:
   decifra()
else:
  print "Digite 1 ou 2!"
  x = raw_input("Escolha a opcao 1 para cifrar ou 2 para decifrar: ")
```